The Framework Programme for Research & Innovation
Innovation actions (IA)

Project Title:
FORTIKA - cybersecurity Accelerator for trusted SMEs IT Ecosystems

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement n°740690

FORTIKA White Paper #3:
The legal aspects of the FORTIKA project: Compliance and best practices

Responsible partner: VUB
Contributing partners: CERTH-ITI, UOM, OBRELA, FINT

Contents

I. Introduction & project overview

Information Technologies are rapidly evolving. They are incorporated into everyday practice in companies of any size in all business sectors. It is difficult to imagine a company that does not use the internet in this day and age. As technology evolves, more and more of company information assets are ported to cyberspace. Operating in a cyber-world means that every company is exposed to cyber threats. As technology evolves, the threats increase in number and become more intelligent, sophisticated and novel. Cyberattacks are the fastest growing crime. Cyber threats comprise a major risk for businesses. It is proven that the vulnerability of a company is inversely proportional to its size. SMEs are typically poorly prepared to defend themselves, their digital assets and their client's data and privacy against cyber threats compared to large enterprises.

The EU-funded project FORTIKA

FORTIKA is an EU funded project under Horizon 2020 program.[1] The project started on the 1st of June 2017 and will end in May 2020. Sixteen partners from nine countries participate in the project, among them three Universities, two Research Institutes, six IT companies and five companies as end users.

The vision of FORTIKA is to develop and test a new technology to minimise the exposure of small and medium sized businesses to cyber security risks and threats. This will help them successfully respond to cyber security incidents, while relieving them from all unnecessary and costly efforts of identifying, acquiring and using the appropriate cyber security solutions. As the cyber-threats become more sophisticated with time, it is required to deploy advanced and effective countermeasures. The FORTIKA approach is to engage artificial intelligence algorithms that watch the company network, identify the threats and initiate the countermeasures.

The **FORTIKA Solution** will be comprised of:

- Hardware, or the **FORTIKA Gateway**,
- Software Services – software packages customized for the FORTIKA Gateway, called the **FORTIKA Bundles,**
- An online marketplace, the **FORTIKA Marketplace,**
- FORTIKA SaaS Software Services.

The **FORTIKA business model**: The FORTIKA hardware with its middleware will be purchased by the FORTIKA clients and installed at client premises. FORTIKA Hardware could be updated with new features using the FORTIKA Marketplace. The FORTIKA Software Services will be provided by the FORTIKA partners. Also, FORTIKA Hardware and FORTIKA Marketplace will be provided by FORTIKA software developers. Additional FORTIKA Services, not implemented during FORTIKA project, could also be made available in the FORTIKA Marketplace. The FORTIKA Marketplace will be run, either collectively or by a single representative of the FORTIKA partners; The FORTIKA solution will be operated and served as professional services under contract and licensing of the different components.

II. What is the applicable legal framework for the FORTIKA solution?

Two legal fields have been identified of direct interest to the FORTIKA project: EU cybersecurity law and EU personal data protection law.

(i) EU cybersecurity law and the FORTIKA solution

The FORTIKA Solution and the EU Cybersecurity Strategy. The FORTIKA project coincides with the EU Cybersecurity Strategy and its central regulatory text, the Network and Information Security (NIS) Directive (Directive EU 2016/1148), which came into force in May 2018. The background of the FORTIKA project is precisely described in the first two recitals of the NIS Directive: “Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market. The magnitude, frequency and impact of security incidents

are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union".

To this end FORTIKA proposes a resilient overall cyber security solution that integrates hardware and software with business needs and behavioral patterns at individual and organizational level. In more detail, a novel marketplace platform, the FORTIKA Marketplace, is introduced; Through this trusted security marketplace, users will be able to transact with Service providers and multiple third-party developers and choose from a number of available security services. The Marketplace will thus enable (third-party) service providers to specify security services and sell or advertise these through a secure and easy to use interface.

Application of the NIS Directive on the FORTIKA Solution. The FORTIKA Solution is considered a Digital Service Provider, and more specifically an online marketplace, within the NIS Directive meaning (Article 4.17), and as such, it must comply with the obligations that the NIS Directive imposes on digital service providers for the security of their network and information systems.

(ii) EU data protection law and the FORTIKA solution

The FORTIKA solution and EU data protection law. The FORTIKA Solution consists of the FORTIKA hardware, that will be installed locally at the enterprise premises and will embed and provide holistic security services tailored to the needs of the FORTIKA clients, while it will have the capability to collect and handle the data of a large number of devices or services (in several of the FORTIKA clients' smart spaces: e.g. business department, shop, industrial environments). The FORTIKA hardware will be connected to the FORTIKA clients' routers. Consequently, it is to be expected that EU personal data protection law will become applicable onto the FORTIKA Solution is a twofold manner: First, the FORTIKA Solution will collect personal data (in the meaning of Article 4(1) of Regulation (EU) 2016/679 – the GDPR) and more specifically data usage data of the clients' personnel or other interacting parties. Second, the FORTIKA Solution will be aimed at protecting the data stored in the FORTIKA clients' premises from cyberthreats; Part (or all) of these stored data may be personal data in the meaning of the GDPR themselves. It is therefore understood that FORTIKA falls within the scope of the GDPR and should therefore comply with its provisions.

III. How does the FORTIKA Solution meet its regulatory requirements?

The FORTIKA consortium has applied a rigorous compliance mechanism in order to warrant compliance of the FORTIKA Solution with its applicable regulatory framework. Work was carried out under the following methodology:

- **Analysis and reporting**

The applicable regulatory framework for the FORTIKA solution has been detailed in a public deliverable report,[2] that was once updated during the project's term[3]. Similarly, the project's pilot cases and business model have been assessed from a legal and ethical point of view (relevant report are not public, to access them please contact the FORTIKA Consortium (https://fortika-project.eu/contact).

- **Project internal compliance mechanisms**

The FORTIKA Consortium has established internal compliance mechanisms, in the format of an Ethics Helpdesk and a Security Advisory Board, that remained operational during the project's term. The Ethics Helpdesk reports are publicly available[4]. If you wish to consult work within the project's Security Advisory Board please contact the FORTIKA Consortium (https://fortika-project.eu/contact).

- **Partner support and guidance**

The FORTIKA Consortium provided support and guidance to the FORTIKA technical partners during the development of the FORTIKA Solution. Support and guidance was provided, most notably, through support during administrative (state) procedures, as well as through development and circulation of questionnaires and checklists. If you wish to consult the relevant forms, please contact the FORTIKA Consortium (https://fortika-project.eu/contact).

- **Data protection by design and by default**

The basic system architecture GDPR principles of data protection by design and by default have been applied rigorously during the development of the FORTIKA Solution. Indicatively: Encrypted communication channels (e.g. TLS) are utilized for securing the exchange of data between the various FORTIKA systems (e.g. FORTIKA GW, FORTIKA Cloud/Marketplace) and components (e.g. FORTIKA security bundles and respective software agents). In addition, Identity and Access management (e.g. Keycloak) is used to control the entities requesting access to the FORTIKA systems and data along with a role based authorisation control (RBAC) scheme for assuring that any entity requesting access to the FORTIKA resources (e.g. data) has the needed privileges.

IV. What do the FORTIKA users need to be aware of? Next steps and implementation checklist

While the FORTIKA Solution has been developed under the highest legal and ethical standards the FORTIKA users need to remain aware of the fact that the FORTIKA Solution does not provide itself compliance with legal (EU) requirements. The FORTIKA Solution is a compliance tool, or add-on, and not legal compliance itself. The FORTIKA users may incorporate it into their business practices, as part of their business routines, and also as part of their compliance exercise with the regulatory requirements outlined above, under I. The FORTIKA Solution is warranted to work seamlessly within each FORTIKA user's legal compliance exercise; However, in a standalone format, while a critical component in its own merit, it does not warrant compliance in full.

In view of the above the FORTIKA users are invited:

- To assess the technical specifications and descriptions of each of the FORTIKA Software Services and Bundles they are interested to purchase against their needs;
- To read carefully the relevant terms and conditions for the provision of the FORTIKA Solution and each of the Software Services and/or Bundles;
- To validate the incorporation of the FORTIKA Software Services and/or Bundles they have purchased through the FORTIKA Marketplace, particular

with regard to interconnection with their internal information technology and electronic communications systems;
- To incorporate the FORTIKA Software Services and/or Bundles they have purchased through the FORTIKA Marketplace within their legal compliance internal mechanisms (particularly with regard to the GDPR and/or the NIS Directive context they may need to alert their DPOs or state authorities, as applicable);
- To remain updated with fixes, patches and updated versions made available to them through the FORTIKA Marketplace; In the same context, to examine and apply any amendments in the FORTIKA Marketplace or other terms and conditions entered by them under the FORTIKA Solution.

The FORTIKA Solution aims to provide a critical operational and legal compliance tool to the FORTIKA users. It can be easily embedded into the corporate mechanisms for legal compliance. Towards facilitating this task, the FORTIKA Consortium based on its experience and specialisation, will provide any guidance and support necessary, on a continued basis, for achievement of the FORTIKA aims and purposes.

DISCLAIMER

This White Paper has been drafted in order to demonstrate the actions carried out by the FORTIKA consortium in order to warrant legal compliance of the FORTIKA project. It does not constitute legal advice, opinion or consultation. FORTIKA users should carry out their own legal assessment prior and during use of the FORTIKA solution. Nothing in this White Paper should be construed as a warranty or undertaking by any partner within the FORTIKA consortium as to the FORTIKA's solution application, merchantability or fitness for any purpose.

V. References

[1] FORTIKA project's official webpage, FORTIKA Consortium, 2017, https://fortika-project.eu

[2] D2.1 – FORTIKA legal and policy requirements, FORTIKA Consortium, 2018, available at the FORTIKA website

[3] D2.6 – FORTIKA legal and policy requirements v.2, FORTIKA Consortium, 2020, available at the FORTIKA website

[4] D2.5 – FORTIKA Ethics Helpdesk Reports, FORTIKA Consortium, 2018, available at the FORTIKA website