Privacy Statement – ECHO Workshops and events

PRIVACY STATEMENT

Information to be provided for workshops and events

(art. 13 GDPR "Information to be provided where personal data are collected from the data subject")

European network of **C**ybersecurity centres and competence **H**ub for innovation and **O**perations.

ECHO delivers an organized and coordinated approach to improve proactive cyber defence of the European Union, through effective and efficient multi-sector collaboration. The Partners will execute on a 48-month work plan to develop, model and demonstrate a network of cyber research and competence centres, with a centre of competence at the hub.

Data controller and Data Protection Officer

RHEA SYSTEM SA (RHEA), established in AVENUE EINSTEIN 8, WAVRE 1300, Belgium, is the Data controller and will manage personal data in compliance with the provisions of European Regulation 2016/679 ("GDPR"), thanks also the establishment of a Privacy Team and the nomination of a DPO (Data Processor Officer).

Data subject can contact the Data Controller and DPO to the following email – address:

Controller Contact: echo.project@rheagroup.com

Data Protection Officer Contact: Jean-Yves Dumoulin:

echo.data.protection.officer@rheagroup.com

Data collected

ECHO is organising a 1-day Spring Seminar "CYBER THREAT INTELLIGENCE IN THE INCIDENT RESPONSE CYCLE ON THE BOARD OF MODERN SHIPS" on 31 March, 2022 with online location using MS Teams.

Learning event is focused on junior specialists and enthusiasts. The training level is not introductory, nevertheless the topics will not be subject to advanced discussions.

Before making a decision on whether you want to participate or not, please read this document carefully. Please ask all the questions you may have so you can be completely sure to understand all the proceedings of the study, including risks and benefits. This informed consent document may include words that you do not understand. If this is the case, please ask the controller or the DPO to fully explain the meaning of

ECHO project has received funding from the European Union's Horizon H2020 research and innovation programme under the grant agreement no 830943

the word or piece of information you do not accurately understand. At all times, we assure the compliance with the current legislation. With your consent, we will collect:

- **Contact data** (last name, first name, email address)
- **Work experience data** (Cybersecurity years of experience, affiliation type, participation to previous ECHO events)
- **Digital material** (photos, videos)

Purposes of the processing

The video recording made during the Spring Seminar will be treated under strict confidentiality. The recordings comply with the ethical and legal standards in the EU (GDPR). The further use of the recordings for learning purposes will not include personal data and such data will not be provided to third party. The feedback of the participants will be anonymized and aggregated, so as to not reveal personal information and identity.

You are asked to participate to Spring Seminar "**CYBER THREAT INTELLIGENCE IN THE INCIDENT RESPONSE CYCLE ON THE BOARD OF MODERN SHIPS**" carried out by members of the Consortium, as part of the following ECHO Project scope:

- WP 2 Multi sector need analysis
  - T2.6: Derivation of ECHO Cyberskill Framework and related trainings
- WP 9 Dissemination, Exploitation and Innovation Management

The activity will be organized in one day divided in two parts – morning with introductory presentations and the afternoon as a simulation of an attack against the ECDIS system of a passenger ship.

In particular, the main goals of this Spring Seminar are the following:

- Provide the participants with basic understanding of cyber security concepts and some specific implications in the maritime industry, especially latest technology and operational developments.
- Provide theoretical overview of the methods and tools that support the incident response and analysis,
- Discuss with participants the indicators of compromise of a cyber-attack against a modern ship and processes on the restoring the navigation system after compromising the communications leveraging the ECHO Federated Cyber Range.

Data protection, confidentiality and privacy policies

Your contact data will be securely stored separately from the questions that you have provided. All data will be kept confidential, stored safely, transcribed and pseudonymised or anonymized.

Responses you give will be recorded. Your recorded data will not include any personal identification; hence it will not be possible to identify your responses afterwards.

ECHO project has received funding from the European Union's Horizon H2020 research and innovation programme under the grant agreement no 830943

The ECHO consortium as a whole as well as each consortium Partner has taken appropriate technical and organizational measures for the protection of personal data processed for the implementation of the ECHO project. Namely:

- Each Partner has appropriate (internal) security and privacy policies in place
- Partners without a security and privacy policy will enforce the security and privacy policy provided by the Data controller
- Each Partner uses state of the art technology/infrastructure and security solutions (firewalls, encryption, backups, etc.) and implements strict access control
- Each partner conducts regular security testing (vulnerability scans, etc.) of its internal infrastructure

Recipients of data collected

Personal data will be collected and handled only by key-personnel of the ECHO project involved in the seminar activities.

Data will not be passed, sold or given in another way to third parties that might use it with other purpose.

The processed video recordings from the event will be publicly available on the ECHO Project website for training purposes, through webinars, but they will not be disclosed to other specific recipients by another means.

Benefits and risks

You will learn more about cybersecurity in the maritime sector. In particular, you will be:

- Trained to interpret the application of the incident response processes in a specific scenario;
- Provided with incident information given in the form of branching scenario, **to interpret the indicators of compromise** in terms of cyber-incident.
- Provided with incident information given in the form of branching scenario, **to locate the affected systems**.
- Provided with incident information given in the form of branching scenario, **to compare the information on the indicators and sketch the possible impacts**.

No risk is foreseen. You are only requested to be available to participate.

You can get more information in the ECHO website: www.echonetwork.eu

Period for which the personal data will be stored

Data will be stored during the project lifetime and 5 years after the project end (as agreed with the EC in the Grant Agreement).

Where does the data reside and where are they transferred

ECHO project has received funding from the European Union's Horizon H2020 research and innovation programme under the grant agreement no 830943

Personal data are stored on servers located within the European Union. In any case, it is understood that the Data Controller, if necessary, will have the right to move the servers even outside the EU. In this case, the Data Controller ensures that the data transfer outside UE will take place in compliance with the applicable legal provisions, also through the provision of standard contractual clauses provided by the European Commission and the adoption of binding corporate rules for intragroup transfers.

Consent

The provision of data and the related processing for the purposes referred above is necessary, but not mandatory, to participate to the Spring Seminar. **Any refusal or missed submitting will lead to the inability to be involved in the Spring Seminar activities.**

Rights of the data subject

You are the data subject of your personal data. The data subject may exercise her/his rights at any time. Specifically, the data subject can ask the data controller to:

- Access personal data;
- Rectify personal data;
- Obtain erasure of personal data.

The data subject is aware of the:

- Right to object to the processing of her/his data;
- Right to withdraw consent at any time;
- Right to lodge a complaint with a supervisory authority.

ECHO project has received funding from the European Union's Horizon H2020 research and innovation programme under the grant agreement no 830943