

ECISO Label

CYBERSECURITY MADE IN EUROPE

Terms and Conditions of Usage

1. Introduction

The ECISO's CYBERSECURITY MADE IN EUROPE Label (hereinafter, the Label) is part of the SME Hub platform developed by the European Cyber Security Organisation (ECISO) as a marketing support and networking tool for the European cybersecurity companies.

In this document, the terms 'Europe' and 'European' are used to denote the European Union Member States (EU27), the European Free Trade Association (EFTA) and European Economic Area (EEA) countries, as well as the United Kingdom (UK).

Purpose. The Label is designed as the industry-driven marketing instrument responding to several critical needs of cybersecurity companies, and small and medium enterprises (SMEs) in particular:

- a. Promote qualified European-based cybersecurity companies and increase their commercial exposure far beyond their traditional home markets.
- b. Raise awareness among users, business partners and investors of the strategic value of cybersecurity companies originating in Europe and driving their business forward based on the trustworthy European values.

Scope. Due to the nature of the Label and its purpose, not all entities involved in the European cybersecurity market are considered eligible for the Label. Under the Label scheme, the European SMEs, large companies, integrators, as well as telecoms and other service providers are considered eligible for the Label:

- **SMEs and Large Companies:** The label targets SMEs primarily, but does not exclude large companies.
- **Integrators:** Large European cybersecurity companies are often both cybersecurity providers and integrators, therefore they can apply for the label if more than 50% of solutions are European.
- **Telecoms and other service providers:** Entities providing cybersecurity services, such as telecoms, MSSPs, consultancies etc, shall be considered cybersecurity companies and therefore be eligible to apply for the Label.
- **Holding and its subsidiaries.** It is also equally important to define the right to use the Label between a holding and its subsidiary companies. According to the Label scheme, if a holding has applied and obtained the label, it can be used only by the holding itself

and not by its subsidiary companies. Likewise, each subsidiary should apply for the Label, even if the holding has one.

2. Key principles

Indicator of trustworthy European origins. The Label is intended to designate the geographic – European – origin of a company and the declaration of conformity with basic security requirements as described in Paragraph 3 of this document. The Label does not claim to measure the quality of its products and services.

The Label is restricted to entities declaring conformity with the criteria and assumptions described in Paragraph 3. As such, the Label is distinct from the certification process and certification schemes which are usually based on the technical audit to verify the quality and functionalities of certified products and services.

Market transparency and self-declaration approach. The Label is based on a self-declaration scheme which is equally applicable to all European countries and is governed by a two-level verification structure.

The first level consists of a network of qualified issuing partners which have signed the partnership agreement with ECSO and have been granted the right to issue the Label. The first level decides whether to issue the Label to the applicants.

The second level is represented by ECSO which is in charge of the general governance and issuing of the Label. ECSO also oversees the administration, communication and the external relations of the Label.

This multiscale verification approach aims to ensure the synergy with the existing national/regional initiatives and to avoid automatic attribution of the Label to unverified companies.

3. Eligibility requirement

The Label is granted to the cybersecurity companies from the European Union (EU27), European Free Trade Association (EFTA) and European Economic Area (EEA) countries, as well as from the United Kingdom (UK), based on the evaluation according to the following criteria:

- a. **European-based:** The company is a legal entity, headquartered in Europe. If the company is a part of a group, then the group headquarters must be registered in Europe.
- b. **European ownership:** The company must provide reasonable assurance (declaring ownership structure, majority stakes) that there is no major ownership/control from the outside Europe.

- c. **Europe as a primary business place:** The company must demonstrate that it has >50% of cybersecurity R&D activities and/or >50% of staff (FTE) located in the EU27, EFTA, EEA countries and the UK.
- d. **Trustworthy cybersecurity (ICT) products and services:** The company declares to comply with the basic requirements defined by the ENISA's „Indispensable baseline security requirements for the secure ICT products and services“¹, including no-spy declaration, which ensures that no offered product or solution contains backdoors (non-declared functionality).
- e. **Data and privacy:** The company declares to be GDPR compliant.

4. Application process

Issuing timeline. The applications for the Label are accepted on a rolling basis. It is recommended that the final decision on the application shall be issued within the period of two months (60 days), which starts on the day when the applying company submits the application to the qualified issuing partner for the evaluation procedure.

Required documents. The Label is issued to companies fully meeting the criteria, which are defined in the application form (see Annex I). Each company applying for the Label shall submit a duly completed application form, as well as the following documents:

- a. Factsheet about the company, including the declaration of the ownership structure, majority stakes and proof of the majority of R&D activities in Europe.
- b. Declaration about the conformity with ENISA's „Indispensable baseline security requirements for the secure ICT products and services“ (including the description for each of the 10 points).
- c. CEO Letter, signed by CEO or any authorised signatory of the company with power of attorney, declaring the correctness of the application form, as well as the Payment Commitment for the processing fee for issuing the Label.

The completed documents must be sent electronically to either the issuing partner of the country where the company has its legal headquarters or to any other issuing partner of its choice. The list of qualified issuing partners is available on the Label website: <https://www.cybersecurity-label.eu/>

5. Verification and approval procedure

The verification and approval procedure are carried out by the qualified issuing partner. In cases, where the evaluation has been carried out by the third-party expert, the qualified issuing

¹ See Annex II and ENISA, ‘Indispensable baseline security requirements for the procurement of secure ICT products and services’, 21 January 2017. Accessible: <https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services>.

partner includes such evaluation into final decision regarding the applicant's compliance with the Label requirements.

After the verification of the eligibility criteria is completed and the payment is received, the applicant shall allow the qualified issuing partner to make all necessary background checks, as well as quality and plausibility review, to verify the content of the self-declaration. Such verification could be made in-house or with the support of an independent third-party expert mandated by the qualified issuing partner if necessary.

During the verification phase, the company for the Label might be contacted to provide more supportive evidence.

The approval procedure is recommended to be carried out in two steps:

- a. First phase.** The receipt of documents and their verification (completeness and plausibility checking) is overseen by the qualified issuing partner and/or by a third-party expert if necessary. The third-party expert have to be an independent consultant with recognised expertise and skills in data analysis and cybersecurity. The qualified issuing partner decides, after consulting with ECSO if seen necessary, whether and in which cases to hire a third-party expert.
- b. Second phase.** Based on the results of the investigation and verification process, the decision to either approve or defer or decline the application for the Label is made by the qualified issuing partner. In cases of suspicious or unclear applications, the qualified issuing partner shall consult ECSO regarding the final decision.

If a qualified issuing partner issues a local/national label according to the equal criteria, for which the applicant already has successfully qualified, then the ECSO Label can be issued with no further checks. Regardless of this, the company needs to fill in the application form to allow the ECSO Label Committee to keep the database up-to-date and pay the Label fee.

6. Issuing procedure

All cybersecurity companies granted the right to use the Label will be published on the Label website. The factsheet or other documentation about the company, including the declaration of the ownership structure, majority stakes and proof of the majority of R&D activities in Europe will not be published publicly.

7. Period of validity

Each labelled cybersecurity company has the right to carry the Label for the period of 12 (twelve) months.² Once the deadline has expired, the reissuing procedure must be performed based on the declaration of the relevant changes to the initial declaration.

² The Labels which have been issued during the launch period (2 November 2020 - 1 March 2021) are exceptionally valid until 31 May 2022.

The holder of the Label commits to inform the qualified issuing partner, as well as ECSO, about any modifications of its capital characteristics or the general terms and conditions of sales, as these modifications might affect the eligibility to the Label. The changes to the criteria described in Paragraph 3. shall be reported within 1 (one) month after the change has taken effect (e.g. change of ownership). Non-reporting of changes affecting the eligibility criteria is considered a breach of the Label conditions and may result in immediate revocation of the Label. Qualified issuing partners bear the right and responsibility to take actions as they see appropriate and proportional to address the potential misuse of the label and the breaches of the eligibility criteria.

Validity of the Label ends when either the issuing period has ended without performing the re-issuing procedure or when any eligibility requirement voids. After the end of validity period, the company lose the right to use the Label both electronically and physically. A grace period of 1 (one) month is granted to remove the Label from all communications.

ECSO maintains an up-to-date list of the valid holders of the label on its website (www.ecs-org.eu), where the status of any company can be checked.

8. Governance

ECSO owns the Label scheme, keeps the database of companies, ensure promotion and marketing of the Label at the European level. As the owner of the Label, ECSO grants the right to the partnering organisations to issue the Label at the local and national level.

European-based organisation willing to become an ECSO partner and issue the Label shall receive the accreditation from ECSO and sign a Partnership Agreement. Only the ECSO accredited organisations will be allowed to issue the Label.

9. Fees

The pricing of the Label is discretionary to the issuing organisations based on their own costs related with the investigation and verification of the applications submitted by the cybersecurity companies applying for the Label, as well as on the membership benefits the qualified issuing partner offers to its members.

For more details please refer to the qualified issuing partner of the country where your company has its legal headquarters or any other ECSO authorised issuing partner.

10. Logo Usage

The usage of the Label is reserved to the companies which receive a formal approval of their application from the qualified issuing partner, based on the criteria identified in this document.

The company, which compliance with the Label criteria are confirmed, receives a non-exclusive and non-transferable right to use the Label for the institutional and communication

purposes (e.g. corporate website, marketing brochure etc), as well as for the general terms and conditions of sale.

The right of usage of the Label is strictly limited to the legal entity which has been granted the right to use the Label and therefore cannot be transferred to a third party (company, institution, federation) under any circumstances. Exceptions are 100% owned subsidiaries which fully comply to the governance of the eligible legal entity including full conformance with eligibility requirements described in the paragraph 3. Such entities shall be listed in the application form.

Companies granted a right to use the logo shall utilise the Label logo in compliance with the following rules:

- a. The logo will appear as provided by ECSO and qualified issuing partner.
- b. The logo will always stand alone and will not be combined with any other graphical elements.
- c. The logo will not be altered in any manner including its size, proportions, font, design, arrangement, colours, or elements or animated, morphed or otherwise distorted in perspective or appearance.
- d. The logo will be displayed in a positive manner and will not be used in any way that adversely affects ECSO Label scheme.
- e. It is understood that the user of the logo shall not acquire and shall not claim any title to the logo which is the subject of this authorisation.
- f. The user shall not register or seek to register any trademark or name which contains the logo, or which is so similar to the logo as to be likely to cause deception or confusion.
- g. The logo will not be used or displayed in any way that disparages ECSO Label scheme, infringes any intellectual property or other rights of ECSO, violates any national or international law, or diminishes or otherwise damages ECSO's goodwill in the logo.

The CYBERSECURITY MADE IN EUROPE Label is a registered trademark and unauthorised usage of it will be legally prosecuted.

11. GDPR compliance

ECSO fully complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) and carries out its activities based on transparency and accountability. Allowing ECSO to implement correctly GDPR is a shared responsibility between the ECSO Secretariat and the associated parties.

In becoming the holder of the Label, each organisation commits to notify the qualified issuing partner and ECSO about the changes in points of contacts (POCs) that could potentially cause breaches in security or GDPR implementation. The company should inform and request the ECSO Secretariat to remove a person from a mailing list and delete its access to the ECSO Registry once this person does no longer work for the company or changes departments that are not following the work of the ECSO.

The information provided in the Label application form will be used solely for the purpose of verification and issuing of the Label.

ECSO operates according to its Data Privacy Policy: <https://www.ecs-org.eu/documents/data-privacy-policy.pdf>. Your data will be stored and treated in accordance with this Policy.

ANNEX I

Application Form

CYBERSECURITY MADE IN EUROPE Label

All fields marked with '' are mandatory*

Thank you for your interest in the CYBERSECURITY MADE IN EUROPE Label. Please proceed by completing this Application Form.

A prerequisite to answer the questions below and to use the ECSO's Label is to read and accept the Terms and Conditions of the Label Usage.

Please send the completed and duly signed Application Form to the qualified issuer of your choice (the list of qualified issuing partners is available on the Label website, [here](#)).

IMPORTANT NOTE: Some additional information might be requested from you as part of the application process to allow the qualified issuing partner to carry out proper evaluation of your application.

Applying as: (please tick one answer*)

Large providers (directly represented) of cybersecurity solutions / services providers	<input type="checkbox"/>
SMEs (as per European Commission definition ¹) solutions / services providers directly represented; Associations composed only by SME, Startups, Incubators, Accelerators - medium sized	<input type="checkbox"/>
SMEs (as per European Commission definition ¹) solutions / services providers directly represented; Associations composed only by SME, Startups, Incubators, Accelerators - small sized	<input type="checkbox"/>
SMEs (as per European Commission definition ¹) solutions / services providers directly represented; Associations composed only by SME, Startups, Incubators, Accelerators - micro sized	<input type="checkbox"/>

¹ NOTE ON SMEs

Staff headcount		Turnover	or	Balance sheet total	
-----------------	--	----------	----	---------------------	--

< 250		≤ € 50 m		≤ € 43 m	
< 50		≤ € 10 m		≤ € 10 m	
< 10		≤ € 2 m		≤ € 2 m	

A) DETAILS OF THE ORGANISATION APPLYING FOR THE LABEL

Full Name of the Organisation*:

Short Name of the Organisation:

Company headquarters registered in:

Postal Address: Street Name or P.O. Box*:

Postal Address: Number*:

Postal Address: Town*:

Postal Code / Cedex*:

Country*:

Internet Homepage:

If your organisation/company belongs to a larger group or is an affiliated company, please give the name of affiliated organisation/company:

VAT Number*:

Billing address

If it is different from the postal address above, please add it here:

Street Name or P.O. Box:

Number:

Town:

Postal Code / Cedex:

Country:

Organisation Profile*: (Short general description of your organisation, at least 5 lines of text)

Cybersecurity Related Activities*: (More specifics on cybersecurity related activities of your organisation, at least 5 lines of text)

B) COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE LABEL USAGE

I declare that:

The company is a legal entity, which headquarters are located in Europe.

- The major ownership of the company and the final beneficiaries are within Europe. There is no majority governance or decision power over the company from entities outside Europe.
- The company has >50% of cybersecurity R&D activities and/or >50% of staff (FTE) located in the EU27, EFTA, EEA countries, as well as the UK.
- The company complies with the basic requirements defined by the ENISA's 'Indispensable baseline security requirements for the secure ICT products and services', including no-spy declaration which ensures that no offered product or solution contains backdoors (non-declared functionality).
- The company is GDPR compliant.

Required complementary document to be attached to the Application Form:

- Factsheet about the company, including the declaration of the ownership structure, majority stakes and proof of the majority of R&D activities in Europe. *Free-form or template with a list of requirements to be provided by the qualified issuer together with the Application Form*
- Declaration about the conformity with ENISA's „Indispensable baseline security requirements for the secure ICT products and services“ (including the description for each of the 10 points)³. *Declaration Form to be provided by the qualified issuer together with the Application Form.*
- CEO Letter, signed by CEO or any authorised signatory of the company with power of attorney, declaring the correctness of the application form, as well as the Payment Commitment for the processing fee for issuing the Label. *CEO Letter and Payment commitment template to be provided by the qualified issuer together with the Application Form.*

ECISO's Cybersecurity Marketplace

Do you want to appear in the ECISO's Cybersecurity Marketplace?	YES <input type="checkbox"/>	NO <input type="checkbox"/>
<p>We offer you an opportunity to be a part of the ECISO's Cybersecurity Marketplace.</p> <p>The ECISO Cybersecurity Marketplace has been designed as a search platform of the European cybersecurity companies, in particular SMEs. The Marketplace provides the possibility to register companies' profiles and present their products and services to potential buyers, business partners and investors. It aims to serve as a comprehensive and up-to-date search platform of the European cybersecurity solutions. The ECISO Cybersecurity Marketplace is currently under the implementation and is planned to be launched in late 2022.</p>		

C) MAIN CONTACT POINT AND REPRESENTATIVE OF THE ORGANISATION

Family name*

First name(s)*

³ ENISA, 'Indispensable baseline security requirements for the procurement of secure ICT products and services', 21 January 2017. Accessible: <https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services>.

Title

Gender* Male Female

Position in organisation*

Department / Faculty / Institute / Laboratory / Group name

Phone*

Email*

Address of the main contact point (if other than 'A')

Street name Number

Town

Postal code / Cedex Country

D) DATA PROTECTION

The information you provide in this form will be used solely for the purpose of verifying and managing your application request to the CYBERSECURITY MADE IN EUROPE Label.

The European Cyber Security Organisation (ECSO), the founder of the Label, and its network of qualified issuers have respective data protection policies and complies with the EU data protection regulations. The ECSO data privacy policy can be found on its website, [here](#).

If you or the individuals listed above later wish to withdraw their contact details, please contact the qualified issuing association you have submitted your application to and/or ECSO Secretariat via secretariat@ecs-org.eu.

I confirm that I am authorised to formally represent my company/organisation or subgroup thereof and have read and agree with the Terms and Conditions of Usage of the Label.

Date*:

Signature of the authorised representative*:

Annex II

**Conformity declaration with
ENISA’s ‘Indispensable baseline security requirements for
the procurement of secure ICT products and services’⁴**

CYBERSECURITY MADE IN EUROPE Label

Principle	Requirement	Fulfilled (yes/no)	Explanation⁵
Security by Design	The provider shall design and pre-configure the delivered product such that functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations.		
Least Privilege	The provider shall design and pre-configure the product according to the least privilege principle, whereby administrative rights are only used when absolutely necessary, sessions are technically separated and all accounts will be manageable.		
Strong Authentication	The product shall provide and support strong authentication mechanisms for all accounts. If authentication is unsuccessful the product shall not allow any user specific activities to be performed.		
Asset Protection	The product shall provide adequate level of protection for critical information assets during storage and transmission.		
Supply Chain Security	The provider shall give means to ensure that the product is genuine, cannot be tainted during operation, and its integrity are warranted		

⁴ ENISA, ‘Indispensable baseline security requirements for the procurement of secure ICT products and services’, 21 January 2017. Accessible: <https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services>.

⁵ Please explain how you fulfil this requirement and, respectively, if you do not fulfil give an explanation why not or why it may not be applicable.

	throughout the product's lifecycle.		
Documentation Transparency	The provider shall offer comprehensive and understandable documentation about the overall design of the product, describing its architecture, functionalities and protocols, their realisation in hardware or software components, the interfaces and interactions of components with each other and with internal and external services, in order to be able to implement and use the product in the most secure way possible.		
Quality Management	The provider shall be able to provide evidence that a managed security by design approach has been adopted, including documented secure software development, quality management and information security management processes.		
Service Continuity	The provider shall guarantee support throughout the agreed lifetime of the product such that the system can work as agreed and is secure.		
EU Jurisdiction	The provider shall accept that all contracts refer to EU Member State law and only EU Member State law and place of jurisdiction in an EU Member State country and only an EU Member State country, including those with subcontractors.		
Data Usage Restriction	The provider shall explicitly declare, justify and document, context and purpose wise, all data collection and processing activities that take or may take place, including relevant legal obligations stipulating them.		