**ILNAS/ANCC/F007**

**Notification of Non-Compliance**

Modifications: periodic review

1, avenue du Swing

L-4367 Belvaux

Tél.: (+352) 247 743 55

confiance-numerique@ilnas.etat.lu

<https://portail-qualite.public.lu>

Contents

[1 Introduction 4](#_Toc196199546)

[1.1 Context of this document 4](#_Toc196199547)

[1.2 Processing of personal data 4](#_Toc196199548)

[2 Non-compliance details 6](#_Toc196199549)

[2.1 Information about the notifier (CAB) 6](#_Toc196199550)

[2.2 Description of the non-conformity 6](#_Toc196199551)

[2.3 Review by NCCA (to be filled in by the NCCA) 8](#_Toc196199552)

[3 Documents to be attached to this notification form 9](#_Toc196199553)

# Introduction

## Context of this document

This form is to be used in case of CAB intents to notify a non-compliance of a European cybersecurity certificate or EU statement of conformity holder (hereinafter, “EU statement of conformity holder”) established in Luxembourg to NCCA.

The vulnerabilities notification and management procedure of ICT services, ICT products, ICT processes and managed security services (hereinafter, “vulnerabilities management procedure”) under the Cybersecurity Act that is applied by ILNAS is described in the procedure ILNAS/ANCC/Pr003 - Notification and Management of Vulnerabilities.

The documents submitted to the NCCA will be reviewed commented and sent to the stakeholders (ENISA, European Commission, NCCA’s from other member states and National accreditation bodies) by the NCCA.

The CAB is responsible for keeping the NCCA up to date concerning the information provided in this notification form.

All the documents relating to the way in which the NCCA operates can be found on the website of ILNAS: [https://portail-qualite.public.lu](https://portail-qualite.public.lu/fr.html)

## Processing of personal data

ILNAS undertakes to respect the confidentiality of the information provided in this form and the supporting documents, in accordance with the 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).

The information submitted via this form will be collected by the NCCA as the body responsible for carrying out supervision activities in accordance with the Cybersecurity Act.

The collection and storage of the data provided via this form is necessary for the supervision of certification holders or EU statement of conformity holders. No further processing of the submitted data will be carried out. The information submitted via this form will only be stored during the time the supervision is ongoing and for a period of 10 years after the supervision has ended.

Any person referred to in this form has the right, at any time, to consult and to rectify the data stored about him/her as well as to obtain a copy of the data, to request its deletion, to ask for its processing to be restricted or to object to the processing of the data. Requesting the deletion of the data, asking for its processing to be restricted, or objecting to the processing of the data may lead to the withdrawal of the certificate or the EU statement of conformity.

For exercising these rights, please contact the NCCA by using the contact details provided in the form. Complaints may also be lodged with the National Commission for Data Protection (CNPD), having its headquarters at 15, Boulevard du Jazz, L-4370 Belvaux. The data protection officer of ILNAS can be contacted via the following e-mail address: dpo@ilnas.etat.lu

# Non-compliance details

## Information about the notifier (CAB)

Name of the CAB:

Reference of the CAB:

(URL from European Commission website)

## Description of the non-conformity

Which company or organisation is concerned?

What kind of service/product/process/manages security service is affected? (please indicate the URL to Enisa certificate website)

When was the non-compliance observed? (please indicate the date)

When was the non-compliance communicated to the manufacturer or provider? (please indicate the date)

Please describe the non-compliance in detail.

Has the CAB issuing the certificate requested the manufacturer or provider for assertions and amendments to be provided within the time frame of 14 days / 30 days for certificates at the assurance level ‘high’ / ‘substantial’ of the CSA, in order to restore compliance?

 [ ]  Yes [ ]  No

If yes, has the CAB accepted or refused them?

 [ ]  Accepted [ ]  Refused

Does the certificate have to be suspended?

 [ ]  Yes [ ]  No

If yes, Please indicate the end date of the suspension.

Has the owner of the certificate been informed at the beginning of the suspension period?

 [ ]  Yes [ ]  No

Does the certificate have to be withdrawn?

 [ ]  Yes [ ]  No

For a confirmed non-compliance:

What are the potentially impacted certified ICT products?

Is there a series of evaluation tasks to be performed on one or more products?

 [ ]  Yes [ ]  No

Has the CB analysed the related impact analysis report?

 [ ]  Yes [ ]  No

If Yes, what was the result of the analysis?

[ ]  Re-emission of certificates [ ]  Notification of non-compliance to manufacturers

Would you like to provide additional information and/or documents relating to your concerns?

 [ ]  Yes [ ]  No

If yes, please indicate the type of information and/or documents you would like to share with us.

Can this document and attached documents be transferred to stakeholders (ENISA, EC, NCCAs from other EU members and NAB)?

 [ ]  Yes [ ]  No

## Review by NCCA (to be filled in by the NCCA)

Report number (NCCA internal reference)

Has certificate been suspended or withdrawn?

 [ ]  Suspended [ ]  Withdrawn

Does the NCCA have to control the identification of potentially impacted certified ICT products?

 [ ]  Yes [ ]  No

Does the NCCA have to control a series of evaluation tasks to be performed by an ITSEF?

 [ ]  Yes [ ]  No

Has the NCCA approved to extend certificates at the assurance level ‘high’ / ‘substantial’ of the CSA, no more than three times the initial length (14 days / 30 days)?

 [ ]  Yes [ ]  No

Does the NCCA agree (if requested by CB and duly justified) to extend the suspension period no more than 3 times the initial length (14 days / 30 days)?

 [ ]  Yes [ ]  No

Does the NCCA decide to extend the suspension period but not more than for a year?

 [ ]  Yes [ ]  No

If ‘Yes please provide a justification (ie: lack of availability of the CB):

Has the NCCA reported the consequences of confirmed non-compliances to the ECCG?

 [ ]  Yes [ ]  No

Remark : The consequences of confirmed non-compliances in the conditions under which the certification takes place and that are not related to the individual ICT product shall be reported by the NCCA to the ECCG.

# Documents to be attached to this notification form

The following documents have to be attached to this form

* The impact analysis report
* Any documents that are deemed relevant to demonstrate the non-conformity of the concerned ICT products, ICT services and ICT processes

Please note that the NCCA might request additional information that it considers necessary for demonstrating the non-compliances with the applicable requirements.

The duly completed and electronically signed request form (File > Info> Protect Document > Add a Digital Signature), together with the documents indicated in Section 3, should be encrypted[[1]](#footnote-1) and emailed to supervision-cybersecurite@ilnas.etat.lu.

1. <https://portail-qualite.public.lu/fr/cybersecurity-act/ncca/contact-ncca.html> [↑](#footnote-ref-1)