

Liechtenstein Country Report



About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports:

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

Internet: <http://www.enisa.europa.eu>



Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: **Dan Cimpean, Johan Meire and Nicolas Roosens.**

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. Member States are not responsible for the outcomes of the study.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA) 2011

Table of Contents

LIECHTENSTEIN	4
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS	4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES	5
OVERVIEW OF THE NIS NATIONAL STRATEGY	5
THE REGULATORY FRAMEWORK	6
NIS GOVERNANCE	8
OVERVIEW OF THE KEY STAKEHOLDERS	8
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	9
FOSTERING A PROACTIVE NIS COMMUNITY	9
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....	10
SECURITY INCIDENT MANAGEMENT	10
EMERGING NIS RISKS AND RESILIENCE ASPECTS	10
PRIVACY AND TRUST	10
NIS AWARENESS AT THE COUNTRY LEVEL	11
RELEVANT STATISTICS FOR THE COUNTRY	12
APPENDIX	13
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY	13
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	13
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	13
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	14
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	14
REFERENCES	14

Liechtenstein

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader on the following Network and Information Security (NIS) related topics:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
 - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
 - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
 - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
 - *Security incident management*
 - *Emerging NIS risks*
 - *Resilience aspects*
 - *Privacy and trust*
 - *NIS awareness at the country level*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

Building upon the success achieved up to now, Liechtenstein's IT and eGovernment Strategy 2011¹ aims to address future challenges with the best possible efficiency. As described also in previous year the strategy targets three main goals which are:

- **Establishing a modern Public Administration and transforming the country into an attractive business location:** the provision of advanced eGovernment services shall be based upon a set of comprehensive and versatile basic services, also called one-for-all services, aimed to providing fundamental functionalities to several Government applications;
- **Fulfilling external requirements:** there are several situations, where the country has to comply with a broad spectrum of IT and eGovernment related requirements, which originate from external institutions. These types of requirements are e.g. those set by the EU within the framework of the "i2010" initiative, or those relating to the implementation of EU directives;
- **Meeting users' needs:** The eGovernment Strategy 2011 aims at addressing users' needs in the most comprehensive way and at achieving an open minded, customer/user oriented and progressive Public Administration, which shall act as a paradigm of innovation and quality for both the public and private sectors.

According to regularly conducted assessments, Liechtenstein consistently achieves a high rate of implementation of EU directives into national law. Liechtenstein's accession to the Schengen and Dublin agreements² requires Liechtenstein's integration with European databases such as the Schengen Information System (SIS)³ and Eurodac⁴. The Liechtenstein's Data Protection Act was totally revised to enable Liechtenstein to join Schengen/Dublin.

To underscore the independence of data protection vis-à-vis the executive branch, the Data Protection Unit will henceforth be subordinate to Parliament. The Liechtenstein Data Protection Commissioner is elected by Parliament, entailing a high level of democratic legitimacy and emphasizing the main purpose of data protection, namely the protection of personality and privacy of citizens as well as legal persons.

¹ Source: <http://www.epractice.eu/files/eGovernment%20in%20LI%20-%20Feb%202010%20-%2008.0.pdf>

² Source: <http://www.liechtenstein.li/en>

³ Source: http://www.europarl.europa.eu/compar/libe/elsj/zoom_in/25_en.htm

⁴ We refer to the following source of information:

http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/133081_en.htm

The regulatory framework

The following regulations of Liechtenstein have relevance and applicability in the domain of Network and Information Security (NIS):

Data Protection/Privacy Legislation⁵

The Data Protection Act

Data security and the right of self-determination are guaranteed by the Data Protection Act of 14th March 2002. The act covers both for private individuals and state authorities and it implements into national law the EU Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

The Data Protection Act was supplemented by two regulations in July 2002 (register number 235.11) and February 2006 (register number 235.111). The latter concerns use of personal data by the police for cases related to terrorism, national security and crime prevention.

No updates in terms of data protection/privacy legislation have been noticed in 2010.

eCommerce Legislation

Law on electronic commerce

The Law on E-Commerce (E-Commerce-Gesetz; ECG, register no. 215.211.7; LGBl. 2003 No. 133) came into effect in June 2003. Among other things, this law implements the European Directive [2000/31/EC](#) on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

No update of the Liechtenstein law on electronic commerce has occurred in 2010.

eCommunications Legislation

The Law on Electronic Communication (Kommunikationsgesetz; KomG, registry number 784.10; LGBl. 2006 No. 91)

The Office of Communication (Amt für Kommunikation) was instituted on 1 January 1999 in Liechtenstein, constituting the regulatory authority for telecommunications services. The legislation for communications was updated in September 2004, by the regulations for mobile telecommunications. On 6 June 2006 came into force the Law on Electronic Communication (Kommunikationsgesetz; KomG, registry number 784.10). This legal framework, concerns the provision of broadcasting services as well as of services of the information society (i.e. online services).

The major update in 2010 is the revision in regard to fraud issues in the national calling range, security measures within telecommunications services and the transposition of the data retention directive 2006/24/EC.

⁵ Source: <http://www.epractice.eu/en/document/288451>. The same source is applicable for other Liechtenstein legislation relevant for NIS.

Cybercrime

Criminal Code

On 17 November 2008 Liechtenstein signed both the Convention on Cybercrime (CETS No. 185) and its Additional Protocol, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189).

Liechtenstein focuses on penal code legislation concerning cybercrime-related offences, such as copyright violations, computer fraud, child pornography and security violations of electronic networks. Elements of offences contained in the convention are planned to be included in the Liechtenstein's penal code.

Since the Liechtenstein Criminal Code is based on the Austrian model, defense measures against cybercrime will be carried out in conformity with the Austrian Criminal Code. The draft law amending the Criminal Code, which the Government has circulated for consultations until the end of 2009, includes a legal definition of the terms "computer system" and "data", in order to prevent legal uncertainties. Unlawful access to computer systems, known as "hacking", will be subject to new criminal provisions. The abusive interception of data will also be punished as a violation of communication secrecy. Disruptions of the functionality of computer systems and the misuse of computer programs will henceforth also be punishable. Data forgery will be subject to sanctions, analogous to traditional forgery of documents. Finally, the production of false data and the falsification of true data are also included as criminal offenses.

No major update or other additional specific law or legal texts regarding information security, electronic delinquency, physical protection or eGovernment have been identified.

Self-regulations

There is currently no public information on a code of conduct adopted by the telecom operators from Liechtenstein. This was the case also in prior years.

eIdentity

General overview

Liechtenstein makes use of a national e-ID card for its citizens. The authentication certificate contained in the e-ID card is issued through a PKI based system, by communes and upon identification in person. It incorporates two certificates: one for encryption and one for electronic signatures (only the latter is considered as qualified).

Additionally, Liechtenstein operates a certain degree of interoperability with Austria, in the sense that certificates issued by ATrust can be used within the National Public Administration.

eSignatures legislation

Law on electronic signature: The current legislation on eSignatures (Signaturgesetz; SigG, registry number 784.11; LGBl. 2003 No. 215) has been in force since September 2003. Among other things the law implements the European Directive 1999/93/EC on a Community framework for Electronic Signatures. It has been supplemented by the regulation on Electronic Signatures in June 2004 (SigV, registry number 784.111).

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	<ul style="list-style-type: none"> Ministry of economic affairs Office for Communications / National Regulatory Authority Stabsstelle für Datenschutz - Data Protection Unit National Authority for the Supervision of Personal Data Processing
CERTs	<ul style="list-style-type: none"> SWITCH-CERT (Switzerland)
Industry Organisations	<ul style="list-style-type: none"> IKT (Platform for Information- and Communications Technology)
Academic Organisations	<ul style="list-style-type: none"> University of Liechtenstein
National Authorities	<ul style="list-style-type: none"> Ministry of economic affairs Office for Communications / National Regulatory Authority Stabsstelle für Datenschutz - Data Protection Unit National Authority for the Supervision of Personal Data Processing

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"⁶ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory⁷.

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, eID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

⁶ The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

⁷ Source: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Co-operation via the Ministry of Economic Affairs and via the Office for Communications

The Liechtenstein, the Ministry of Economic affairs (formerly the Ministry of Transport and Communications) is currently responsible for the development of electronic communication policy. Its body, the Office of Communications, is the national regulatory authority with the tasks of monitoring responsibilities in electronic communications, and administrative responsibilities of frequencies, numbering and identification resources.

Liechtenstein is committed to data protection and ensuring compliance in this regard. The Data Protection Unit is an independent oversight body responsible for this task. It is in charge of supervision of both the protection of personal data, as well as access to public information. The tasks include maintaining a register of databases, investigating complaints, imposing fines for violations, conducting audits and providing consultations on data protection, and commenting on legislative proposals.

Fostering a proactive NIS community

As it was the case of the previous year, in 2010 no relevant information was available concerning Liechtenstein, from public sources.

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

During the course of 2010 SWITCH-CERT continued to help companies in both Switzerland and **Liechtenstein** to protect themselves efficiently against the misuse of data and internet attacks. SWITCH-CERT operates during the office hours.

The Cybercrime Coordination Unit Switzerland (CYCO) is the central Swiss contact point for people who would like to report suspicious Internet content. After an initial check and back-up, the reports are forwarded to the competent prosecution authorities at home and abroad. On the basis of an agreement with the Liechtenstein national police force, CYCO now also provides its services for the benefit of the Liechtenstein principality.⁸

No specific network or information security incident information is published on the web site of Telecom Liechtenstein – the main telecommunication provider.

Emerging NIS risks and resilience aspects

As it was the case of the previous year, in 2010 no relevant information was available concerning Liechtenstein, from public sources.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the Data Protection Act (collectively the "DPA") dated 14 March 2002 and the relevant Ordinance on the Data Protection Act (Data Protection Ordinance) dated 9 July 2002.

The competent national regulatory authority on this matter is the Liechtenstein Data Protection Commissioner ("Datenschutzbeauftragter").

Personal Data and Sensitive Personal Data

The definition of personal data in the DPA is based on the standard definition of personal data. However, the DPA defines personal data as being all information relating to an identified or identifiable person (i.e. both natural and legal persons).

Sensitive personal data includes: (i) the standard types of sensitive personal data (though this does not include trade union information); (ii) social security files; and (iii) criminal or administrative proceedings and penalties.

The processing for "personality profiles", which is a collection of data that allows the appraisal of fundamental characteristics of the personality of a natural person, is also subject to additional controls.

⁸ Source: <http://www.bakom.admin.ch/themen/infosociety/01691/01710/index.html?lang=en>

Both sensitive personal data and data constituting a personality profile are the subject of specific rules. A private sector entity may only process sensitive data if the standard conditions for processing sensitive personal data are satisfied.

A public sector entity may only process sensitive personal data if: (i) it is indispensable in order to fulfil a specific legal obligation; (ii) the Government has authorised the processing; or (iii) the data subject has granted express consent or made the information public.

The main change identified in 2010 is the transposition of the Directive of Data Retention on public communications networks 2006/24/EG.

Information Security aspects in the local implementation of the Data Protection Directive

Data controllers must comply with the general data security obligations.

Data protection breaches

The DPA does not contain any obligation to inform the Data Protection Commissioner or data subjects of a security breach. However, data controllers in certain sectors may be required to inform competent regulators of any breach.

Enforcement

The Liechtenstein Data Protection Commissioner can investigate cases on his own initiative or at the request of third parties. For this purpose he may request the production of documents, obtain information and have data processing activities explained to him. On that basis the Data Protection Commissioner may recommend improvements and in some cases he also may inform the government about such recommendations.

However, civil procedures and prosecutions for criminal offence can only be carried out by the Princely Court of Liechtenstein.

NIS awareness at the country level

Awareness actions targeting the consumers/citizens and the industry

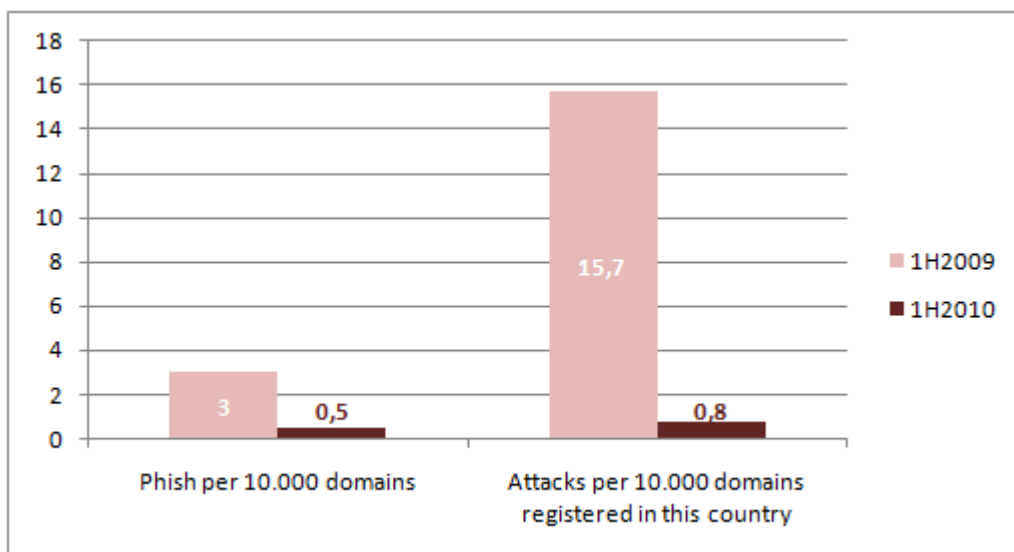
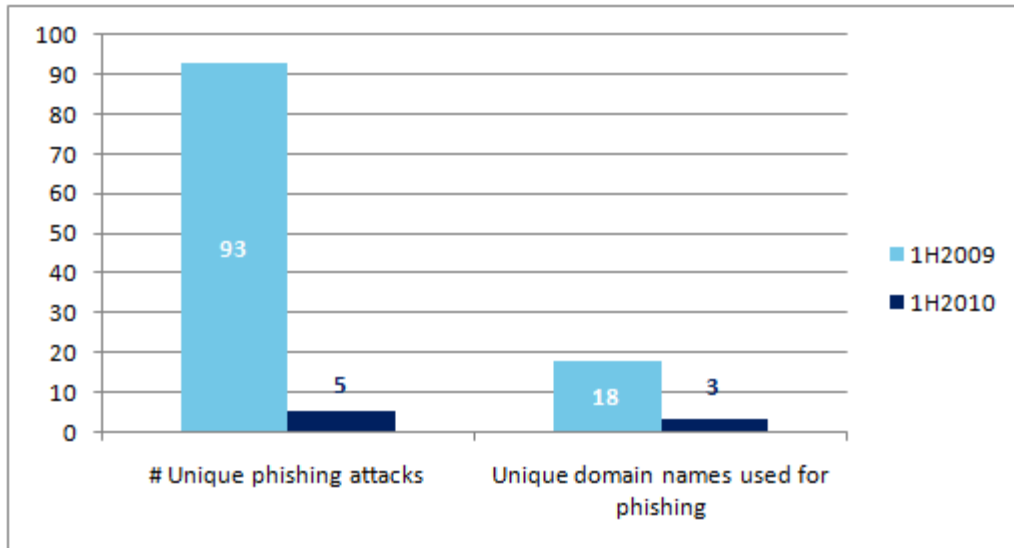
SWITCH-CERT keeps updated the security stakeholders in Liechtenstein (in addition to Swiss stakeholders) on the current risk situation in the Internet in order to help implement the correct protective mechanisms against cyber attacks and to notify the customers concerned. In addition, undertakes actions to increase the in-house IT security awareness of users.

SWITCH-CERT offers companies a comprehensive service package, suitably tailored to their specific sector, which can be individually aligned to their needs: from "forensic analysis" via the controlled simulation of a cyber attack, and from the selective tracking down of potential malware through honeypot traps through to in-house training courses.

Malicious software programs such as Trojan horses, viruses and worms are monitored and analysed by the CERT team, in SWITCH's own security laboratory.

Relevant statistics for the country

It is interesting to mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Liechtenstein was mentioned in the global report⁹ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



Unfortunately we notice here that no details statistics are available on Eurostat as it is the case for many other countries.

⁹ See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

APPENDIX

National authorities in network and information security

National authorities	Role and responsibilities	Website
1. Ministry of economic affairs	The key responsibilities of the Ministry of Transport and Communications are: <ul style="list-style-type: none"> • Development of electronic communication policy • Monitoring responsibilities in electronic communications • Administrative responsibilities of frequencies and numbering. 	http://www.liechtenstein.li/en/eliechtenstein_main_sites/portal_fuerstentum_liechtenstein/fl-staat-staat/fl-staat-regierung/fl-staat-regierung-verteilung/fl-staat-regierung-verteilung-wirtschaft.htm
2. Office for Communications / Amt für Kommunikation (AK) (AK)	The Office for Communications is the national regulatory authority that has monitoring responsibilities in electronic communications, administrative responsibilities for frequencies, numbering and identification resources.	www.ak.llv.li
3. Stabsstelle für Datenschutz - Data Protection Unit	The Data Protection Unit is responsible to ensure compliance with data and privacy protection policy. The main tasks are: <ul style="list-style-type: none"> • Supervision of both the protection of personal data, as well as access to public information; • Maintaining a register of databases, investigating complaints, imposing fines for violations, conducting audits and providing consultations on data protection. 	www.dss.llv.li/
4. National Authority for the Supervision of Personal Data Processing	The National Authority for the Supervision of Personal Data Processing is responsible for the e-Government strategy of Liechtenstein, and central IT provider for the government. Main tasks: <ul style="list-style-type: none"> • Keep up to date with the newest trends in e-Government; • Define the e-Government strategy of Liechtenstein. 	www.llv.li/amtstellen/llv-apo-home.htm

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
5. SWITCH-CERT	Switch ensures that all domain names ending in .ch or .li are correctly issued and administered. <ul style="list-style-type: none"> • FIRST¹⁰ member • TI11 listed 	www.switch.ch/cert

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
6. IKT (Forum für Informations- und Kommunikationstechnologie in Liechtenstein)	This industry organization is a forum/platform that is mainly active in: <ul style="list-style-type: none"> • Get companies together and help them on ICT matters; • To discuss about the new industry trends; • The organization of 2-3 events a year. 	www.ikt.li

¹⁰ Source: <http://www.first.org/members/teams/>

¹¹ Source: <http://www.trusted-introducer.nl/>

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
7. University of Liechtenstein	Bachelors and Masters programs and continuing education. The Institute for Business Information Systems is a member of the European Research Center for Information Systems (ERCIS) and represents the Association for Information Systems (AIS) in Liechtenstein through the Liechtenstein Chapter of the AIS (LCAIS).	www.hochschule.li www.uni.li

Other bodies and organisations active in network and information security

No other types of relevant organisations dealing with the NIS matters have been identified in Liechtenstein during the desk research.

References

- An overview of the eGovernment and eInclusion situation in Europe, available at <http://www.epractice.eu/en/factsheets>
- ENISA, Information security awareness in financial organisation, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- World Telecommunication/ICT Indicators Data - International Telecommunications Union source of data at: <http://www.itu.int/ITU-D/ict/statistics/>
- See <http://www.liechtenstein.li>

