Explanatory notes to Domain Name Regulation 68

MPS Domain Name Regulation 68

CONTENT

PART A Key changes

This section describes the key changes in Regulation 68 with respect to previous regulations on domain names.

1 Changes

This is the first version of Regulation 68. The Regulation was consolidated from the following previous regulations:

- Regulation 37 E/2006 M on the technical configurations and permitted characters for fi-domain names
- Regulation 52 A/2006 M on the technical configurations and permitted characters for ax-domain names

Regulations 37 E/2006 M and 52 A/2006 M shall be repealed by new Regulation 68 as the amendments based on the Information Society Code (917/2014) [1] enter into force on 5 September 2016. The regulations to be repealed concern the configuration of name servers to serve domain names, email connections, requirements concerning SOA (Start of Authority) records and the domain name length and permitted characters. The requirements of the regulations to be repealed are incorporated in the new Regulation almost in their entirety. However, some changes have been made to these requirements:

- The obligation included in section 2 of the Regulations to be repealed that requires the name servers of a domain name to be reported has been removed due to amended legislation. However, if the name servers are reported, they must be configured in accordance with Regulation 68.
- The new Regulation no longer contains provisions for email connections.
- In Regulation 68, provisions concerning the form of *fi*-domain names are directly extended to cover domain names that end with *ax*. Therefore, the possibility to use national characters associated with the Sami language must now also apply to domain names that end with *ax*.
- The Regulation no longer requires that the serial numbers and timers of SOA records cannot essentially differ from published internet standards and recommendations. This requirement previously included in the Regulation has been changed into a recommendation in this document.

The new Regulation 68 contains a number of provisions that have existed before, but the changes incorporated in the Information Society Code that apply to the regulation of domain names have an impact on the Regulation. The Information Society Code introduces new obligations for domain name registrars. The Act provides for a new operating model in which the domain name must be acquired from a chosen domain name registrar. As the domain name registrar also administers domain names on behalf of the

holder, the Act lays down explicit obligations for the registrar. In addition, pursuant to new provisions of the Information Society Code, the registrar shall ensure the information security of its operations and report any significant disturbances to the authority in charge of domain names.

The new obligations are laid down in sections 2, 4 and 5 of Regulation 68. Regulation 68 provides the following:

- Chapter 2 provides for the various obligations of the domain name registrar (notifications of engagement in domain name registration and its termination, changes to the information provided, notifications of prohibitive decisions of the authority in charge of domain names, obligation to advise holders, information of the holder to be entered in the domain name register, interface with FICORA's domain name register, transfer of domain names to another holder and switch of domain name registrars);
- Chapter 3 provides for the technical specifications of a domain name (domain name form and the configuration of optional name servers);
- Chapter 4 provides for the information security management by a domain name registrar;
- Chapter 5 provides for the obligation to notify information security disturbances.

2 Impacts

The most important change in the Regulation aims at specifying the obligation of domain name registrars referred to in section 170(1)(6) of the Information Society Code. The obligation in question states that domain name registrars must ensure the information security of their operations.

2.1 Impact on the information society

The particular aim of this Regulation is to make a positive impact on the information society by promoting information security in the domain name registrars' operations and thus safeguarding an up-to-date and secure maintenance of the domain name register and the roots *fi* and *ax*. This Regulation also has several positive effects on the holders obtaining domain names as the Regulation specifies the content and quality of the services provided by registrars.

The Regulation contains specific provisions on the information that a domain name registrar shall provide to the authority in charge of domain names. Furthermore, the Regulation specifies the obligation to provide advice referred to in the Information Society Code that contains requirements concerning the content and form of the domain name. The Regulation also specifies the procedures that a registrar must follow when a holder wants to transfer its domain name to another holder or switch registrars. Therefore, the Regulation can be assessed to improve the position of holders and clarify the role of registrars.

The Regulation can be assessed to improve information security in the registrars' operations since it describes the obligation to ensure information security laid down in the Information Society Code in as much detail as possible. On the other hand, the Regulation is flexible since in practice, operators can decide themselves how they comply with the obligations referred to in the Regulation to achieve the desired outcome. The Regulation can be assessed to reduce disturbances in information security since it describes the registrars' requirements to ensure information security in their operations in sufficient detail. Therefore, the Regulation can be assessed to have a positive impact on the information society also in this regard.

2.2. Economic impact

There is no fee for acting as a registrar. Unlike in many other country-code registers, the Information Society Code does not impose any fee for those acting in as domain name registrars. The information security obligations provided in the Information Security Code and specified in FICORA's Regulation may have cost implications for domain name registrars. Complying with the information security obligations can be assessed to cause additional costs for many domain name registrars especially at the early stages of their operations. On the other hand, it must be noted that some registrars have already taken information security issues well into account which means that the existing capacity to comply with the Regulation does not cause additional costs and the economic impact is small.

The Regulation aims at specifying the information security obligations provided by law but the operators may decide themselves how they will comply with the obligations of the Regulation in the most cost-effective way. There are many ways to ensure information security. The nature of the registrar's operations also affects the requirements for information security. A registrar may either use FICORA's browser-based user interface or EPP interface. The latter may have larger cost implications with regard to information security as the registrar's systems connected to the EPP interface must meet the criteria of protection level (IV) of Katakri (information security auditing tool) with respect to data communications security and security of information systems.

The Regulation has been prepared by a working group in cooperation with operators in the field and other stakeholders. Possible cost effects have come up during the consultation of the Regulation but no cost estimates have been presented as such in the comments.

It is difficult to estimate the cost effects of complying with the obligations in the Regulation because domain name registrars differ from one another. The organisations of some operators (such as telecommunications operators) are already subject to statutory obligations related to information security and therefore, new obligations imposed for them as domain name registrars do not necessarily cause material additional costs.

It can also be stated that any costs resulting from the Regulation will be higher at the early stages than in the long term. As the knowledge of information security and information systems have been brought to the required level, maintaining and developing the systems and information security culture will not cause such costs anymore as at the early stages.

It is very difficult to estimate the amount of direct costs resulting from the Regulation in euros. It shall also be noted that obligations concerning information security, as well as other obligations, are provided by law and the Regulation only specifies the requirements imposed by law. The intention has been to minimise the administrative burden of the Regulation by using the stakeholders' expertise throughout the preparation. Taking the above-mentioned issues into account, it may be considered that the Regulation does not impose such obligations on domain name registrars that would cause operators material additional costs. The obligations are fit for purpose and absolutely necessary for attaining the objective of the Information Society Code and the Regulation. When considered as a whole, it may be concluded that the Regulation may cause short-term additional costs for domain name registrars but in the long term, it may be predicted to bring savings as fewer disturbances in information security, for instance. The investigations and damage caused by disturbances in information security also impose costs. Preventive information security measures can be assessed to bring savings in the long term.

2.3. Other impacts on registrars

The obligations of the Regulation are also binding on authorities if they are registered as domain name registrars. The obligations probably require similar changes to the technical systems, operational processes and personnel resources from authorities as from other registrars. However, it may be assessed that the impacts of the Regulation do not impair the authorities' ability to operate within their resources.

The Regulation has some impact on FICORA's activities since it is FICORA's duty to supervise that the Information Society Code and the Domain Name Regulation are observed. However, the Regulation does not have an impact on the human resources within FICORA's supervision duties.
The Regulation does not have a noteworthy environmental impact or significant other social impacts.

PART B Section-specific basis and guidelines for application

Chapter 1 General provisions

This chapter explains Chapter 1 of the Regulation, i.e. the general provisions of the Regulation.

1 Section 1 Objective of the Regulation

Section 1 of the Regulation describes the objective and principles of the Regulation. The provisions of the Regulation aim at achieving these objectives, and the objectives guide the application of the Regulation. The objectives described under section 1 should be considered as a starting point for all operations related to the registration of domain names.

Pursuant to section 1 of the Regulation, its purpose is to:

1) safeguard an up-to-date and secure maintenance of the domain name register and the roots *fi* and *ax;*
2) safeguard an access by domain name holders to information on the requirements concerning the form and content of domain names;
3) promote smooth transfer of domain names or switching of registrars;
4) promote the functioning of domain names;
5) safeguard information security in the registration of domain names;
6) ensure that the authority in charge of domain names is informed about disturbances to the information security of registration operations.

The purpose of the Regulation is to define the minimum requirements concerning the implementation of information security measures. The Regulation is intended to make information security issues part of the everyday operations of domain name registrars. In other words, the Regulation is designed to ensure that factors affecting information security are routinely addressed with effective processes as part of domain name registration operations.

Pursuant to section 3(1)(28) of the Information Society Code, *information security* means the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data and information systems can be used by those who are entitled to use them. In other words, information security covers the measures taken to safeguard the confidentiality, integrity and availability of information. The purpose of this Regulation is to contribute to the realisation of these objectives.

2 Section 2 Scope of application

Section 2 of the Regulation deals with the scope of application of the Regulation. Regulation 68 applies to domain names that end with *fi* or *ax* and to the registration and management of such names.

The requirements of the Regulation have been divided under five topics:

- Chapter 2 deals with certain requirements concerning domain name registrars;
- Chapter 3 deals with technical requirements concerning domain names;
- Chapter 4 deals with specific requirements concerning the management of information security by domain name registrars;
- Chapter 5 deals with the obligation to notify information security disturbances.

2.1 Domain names ending with *fi* or *ax*

Pursuant to section 3(1)(35) of the Information Society Code, *domain name* means second-level address information on the internet under the national country code Top Level Domain .fi or the region code Top Level Domain .ax consisting of letters, digits or other characters or their combination in the form of a name.

2.2 Registration and management of domain names

Registration of domain names means making entries in the domain name register. Pursuant to section 164(2) of the Information Society Code, only an operator who has made a domain name notification referred to in Section 165 of the Information Society Code (*domain name registrar*) may make entries in the domain name register. Pursuant to section 167(1) of the Information Society Code, a domain name shall be registered in the domain name holder's name, and the domain name registrar shall enter into the domain name register the domain name holder's correct, up-to-date and identifying information, as well as the email address to be used for hearing and service of notices

The administration of a domain name covers all operations by a domain name registrar to maintain the information of a domain name entered in the domain name register. For example, section 170(1)(2) of the Information Society Code requires that a domain name registrar shall keep the data in the domain name register up-to-date, while subsection 1(5) of the provision requires that a domain name registrar shall remove a domain name from the domain name register upon request by a domain name holder prior to its expiry date (termination). The administration of a domain name also means the ability to enter data in a domain name register using the technical systems prescribed by FICORA and the ability to ensure the information security of its operations.

2.3 Domain name holder

Pursuant to section 164(3) of the Information Society Code, a *domain name holder* may be a legal person, a business operator or other association or a natural person to whom a domain name may be registered.

2.4 Domain name register

Pursuant to section 164(1) of the Information Society Code, a *domain name register* means a public register maintained by FICORA of domain names ending with the fi-code, and a fi-root means a database of the technical data of domain names for directing internet traffic. The ax-domain name register and the ax-root are maintained, in accordance with the present practice, by the Provincial Government of Åland based on a consentaneous decree provided for in section 32 of the Act on the Autonomy of Åland (1144/1991).

2.5 Scope of application of the Regulation on domain names ending with *ax*

Under section 2 of the Regulation, it also applies to domain names that end with *fi* or *ax* and to the registration and management of such names. However, FICORA notes that provisions of section 9 contain differences between domain names that end with *fi* and those that end with *ax* with regard to domain name registrars' technical interfaces to domain name registers. A domain name registrar registering and managing domain names that end with *fi* may enter domain names into FICORA's domain name register by using FICORA's EPP interface. If the domain name registrar uses FICORA's EPP interface as the technical interface, it must meet the Katakri criteria concerning information security as provided in section 20 of the Regulation. When registering and managing domain names that end with *ax*, the only technical interface available, at least for the moment, is a browser-based user interface at www.whois.ax.

If necessary, the Regulation may be supplemented later with regard to technical interface definitions concerning the registration and management of domain names ending with *ax*.

Pursuant to section 163(1) of the Information Society Code, Chapter 21 on domain names applies to internet domain names that end with the region code Top Level Domain of Åland (region code ax) as well as to domain name administration and provision of domain names. Under section 163(2), the provisions regarding the domain name register maintained by FICORA shall also apply to the register of domain names ending with region code ax. According to the preparatory material related to this provision, the transfer of competence between the State and the Province of Åland to administer the code ax should be provided for in a separate consentaneous decree in accordance with the present practice.

The preparatory material of the Information Society Code also states that with respect to region code ax, the notification by a domain name registrar of launching its registration operations provided for in section 165(1) of the Information Society Code shall be submitted to the Provincial Government of Åland.

In its opinion (18/2014 vp – HE 221/2013 vp), the Constitutional Law Committee stated that in matters falling under the legislative power of the State, a State authority is, as a rule, competent also in Åland. However, the administrative tasks of such an authority may be delegated to the provincial administration by a consentaneous decree referred to in section 32 of the Act on the Autonomy of Åland. Therefore, the registry tasks referred to in section 163(2) of the Information Society Code could be delegated from FICORA to the Provincial Government of Åland only by a consentaneous decree mentioned in the preparatory material of the proposal. With respect to the code ax, the authority in charge of domain names referred to in section 165(1) of the Information Society Code means the Provincial Government of Åland.

2.6 General limitations to the scope of the Regulation

As the Information Society Code does not apply to other top-level domains and the associated domain name operations, they do not belong to the scope of application of this Regulation. Other top-level domains include generic domains, such as .com or .net, or country-code domains, such as .se for Sweden.

3 Section 3 Definitions

Section 3 of the Regulation lists the definitions of the Regulation. The Regulation does not redefine concepts that have been defined in the Information Society Code. On the other hand, the definitions have been drawn up to avoid conflict with the definitions provided for in the Information Society Code. Definitions of the Information Society Code were described above in the paragraph dealing with section 2.

3.1 Domain holder transfer key

A domain holder transfer key means a code defined by the authority in charge of domain names (FICORA or the Provincial Government of Åland) that enables the transfer of a domain name from one holder to another.

3.2 Registrar transfer key

For the purposes of the Regulation, a registrar transfer key means a code that enables the administration of a domain name to be transferred from one domain name registrar to another. As a rule, the code is created by the old registrar. In exceptional cases, the authority in charge of domain names may create the code, if the old registrar, for some reason, fails to meet its obligations under the Information Society Code.

3.3 Old domain name registrar

For the purposes of the Regulation, the old domain name registrar means the registrar relinquishing the administration of a domain name when a domain is transferred from one registrar to another.

3.4 New domain name registrar

A new domain name registrar means the registrar assuming the administration of a domain name when a domain is transferred from one registrar to another.

Chapter 2 Requirements concerning a domain name registrar

Chapter 2 of the Regulation contains provisions on the obligations of domain name registrars concerning notifications and the provision of

advice, the identifying information to be entered in the domain name register, requirements concerning interface with the domain name register and the procedures related to transferring domain names and switching domain name registrars.

4 Section 4 Information to be disclosed in the notification concerning engagement in domain name registration

Section 4 of the Regulation lays down further provisions on the identifying information that a domain name registrar must provide to the authority in charge of domain names before launching its operations. In accordance with the preparatory material of the Information Society Code, the authority in charge of domain names practically means FICORA for the country code fi and the Provincial Government of Åland for the region code ax.

Pursuant to section 165(1) of the Information Society Code, a domain name registrar shall submit a notification to the authority in charge of domain names before launching its operations. The notification shall include the service provider's identification and the email address used for hearings and service of notices, as well as other information relevant for supervision.

Pursuant to section 4 of the Regulation, the notification concerning engagement in domain name registration to be issued to the authority in charge of domain names must include, in addition to an email address laid down in section 165 of the Information Society Code ("address for service"), the following information:
1) name of the domain name registrar;
2) business identification number or personal identity code of the domain name registrar or, if these do not exist, other identifying information;
3) postal address of the domain name registrar;
4) phone number of the domain name registrar;
5) name of the contact person of the domain name registrar;
6) phone number of the contact person of the domain name registrar;
7) email address of the contact person of the domain name registrar.

Section 4 of the Regulation begins with a specification of the identifying information and the contact information required for the notification concerning engagement in domain name registration. These include the name of the domain name registrar, the business identification number of a company or an organisation or the personal identity code of a natural person. If the company does not have a Finnish business identification number, valid identifying information may be another registration number or similar. Since foreign natural persons do not necessarily have a Finnishpersonal identity code, other identifying information in this context means a birth date. Other information to be notified includes any address details necessary for reaching the legal or natural person concerned, the names of contact persons and the contact information of the contact persons. Most of the information to be notified is listed in the preparatory material of section 165 of the Information Society Code.

FICORA notes that the Personal Data Act (523/1999) is a general law on processing of personal data. Provisions of the Act apply to all processing of personal data unless other acts contain corresponding specific provisions. The Personal Data Act also brought into force the Data Protection Directive of the European Union. Several acts on different subjects also contain specific provisions on processing of personal data. They may concern, for instance, the right to collect and record personal data, the right to disclose or store personal data, or the contents of a personal data file. Regulations of the European Union may also contain provisions that are directly applicable to the processing of personal data or that affect such processing. The Act on the Openness of Government Activities (621/1999) applies to disclosing of personal data from a personal data filing system controlled by an authority, unless otherwise provided for a specific function. Processing of personal data is also subject to provisions on secrecy and the principles of good information management. The Data Protection Ombudsman steers and supervises the enforcement of personal data legislation. More information about personal data regulation and the data protection reform to be completed in 2018 is available on the website of the Data Protection Ombudsman at www.tietosuoja.fi.

FICORA notes that all registrars of domain names that end with *fi* or *ax* are obliged to comply with personal data legislation, as applicable, in the processing of personal data. FICORA also states that it is an administrative authority that is subject to other regulation on Government activities such as the Administrative Procedure Act (434/2003). The Act on the Openness of Government Activities applies to disclosing of personal data from FICORA's domain name register. Publishing information on the domain name register on FICORA's internet pages is regulated in section 167(2) of the Information Society Code.

4.1 Statutory address for service and other email addresses

Section 312(2) of the Information Society Code provides for FICORA’s unconditional right to use the email address entered in the domain name register for hearings and service of notices, which means that documents or decisions related to domain names may always be issued by email. This “address for service” has major legal importance, and its notification to the authority in charge of domain names is, under section 165 of the Information Society Code, mandatory to the domain name registrar. For this reason, section 4 of the Regulation refers to the mandatory provision of the Information Society Code. The use of address for service enables FICORA to quickly issue its binding decisions, since pursuant to section 312(2) of the Information Society Code, a decision or other document is deemed to have been received the third day after the sending of the message, unless provided otherwise. The correctness of a domain name registrar’s address for service is important information, and it is very important for the legal protection of the registrar to keep it up to date.

Neither the Information Society Code nor the Regulation prevents the notification of email addresses other than those intended for official hearings or notices. It is possible to notify other email addresses to FICORA's online system, if the domain name registrar considers it necessary to keep email addresses intended for processing everyday technical issues related to the domain name separate from the mandatory address for service. However, the Information Society Code only provides for one mandatory email address.

4.2 Notification of changes in information

Pursuant to section 165(2) of the Information Society Code, the domain name registrar shall notify FICORA without delay of any changes in the information previously notified. According to the preparatory material related to this provision, domain name registrars should report any changes in the information immediately. FICORA recommends that domain name registrars report changes to the database maintained by FICORA within three (3) days.

5 Section 5 The form of the notification and its submission to the authority in charge of domain names

Section 5 of the Regulation provides for the submission of the notification concerning the launch of operations referred to in section 165(1) of the Information Society Code. In addition, this section concerns the notifications of changes in the information provided by domain name registrars. Pursuant to section 5, notifications regarding the fi-domain names must be made through an online service maintained by FICORA at www.ficora.fi, whereas notifications regarding domain names ending with ax must be made at www.whois.ax.

Those making a notification concerning the launch of operations can access the basic details of all rights and obligations of domain name registrars through FICORA's online system, as provided for in the Information Society Code and FICORA's Regulation. At the time of making the notification, potential domain name registrars have the opportunity to familiarise themselves with statutory rights and obligations concerning the operations to be notified. To ensure the awareness of potential and existing operators on the rights and obligations concerning their operations, information is available also on FICORA's website.

A list of operators who have registered as domain name registrars is maintained through publishing the basic details of these operators on FICORA's website. Basic details include the general information of an operator as well as its identifying information. The objective is to make it easier to obtain up-to-date information on operators, which is deemed necessary particularly from the point of view of end users.

FICORA discloses other information defined in section 4 of the Regulation as provided for in the Act on the Openness of Government Activities (621/1999).

6 Section 6 Notifications to customers on changes in the operations of the domain name registrar

Section 6 of the Regulation lays down further provisions on the notifications that a domain name registrar is obliged to make to its customers if it terminates its operations or if it has been notified of a decision by the authority in charge of domain names that prohibits the domain name registrar from operating for up to one year.

Section 6(1) of the Regulation provides that notifications concerning the termination of operations by the domain name registrar must be made on a customer-by-customer basis to ensure that customers actually receive the information. Therefore, communicating the information only through the domain name registrar's website cannot be deemed as adequate, even if it is advisable to publish this information also on the website. With email addresses of the domain name registrar's customers, it is possible to target the notifications effectively, but it may also be necessary to attempt to reach the customers by phone.

Pursuant to section 165(2) of the Information Society Code, a domain name registrar shall inform FICORA and its customers no less than two weeks in advance of terminating operations. According to the preparatory material of the provision, domain name registrars should inform both FICORA and their customers also in cases where their operations are temporarily suspended. Similarly to what has been provided in the preparatory material of the Act for the notifications concerning the launch of operations, also notifications concerning the termination of operations with regard to the region code ax are made to the Provincial Government of Åland. The purpose of the provision is to safeguard the possibility of domain name holders to keep their domain names operable and ensure that domain name holders have enough time to switch domain name administrators before the domain name registrar terminates its operations. FICORA recommends that domain name registrars should make known even temporary suspensions of their operations, for reasons mentioned in the preparatory material of the Information Society Code.

Section 6(2) of the Regulation obliges a domain name registrar to make notifications on a customer-by-customer basis even in cases where its operations are temporarily suspended due to a prohibitive decision by the authority in charge of domain names. Pursuant to section 171(2) of the Information Society Code, if the domain name registrar violates the Information Society Code or the rules, regulations or decisions issued by virtue of it, FICORA may forbid the domain name registrar from entering domain names or changes related to them in the domain name register. Under the provision, such a prohibition is preceded by a note and a

potential decision by FICORA, obliging the domain name registrar to remedy its defect or neglect within a reasonable time period.

According to the preparatory material of the provision, the prohibitive decision would be appealable and it would be practically implemented by preventing the registrar from making entries in the domain name register or editing them through the technical interface. In such situations, the customers of a domain name registrar have to find a new registrar, which means that the obligation of the registrar to inform its customers is an important minimum requirement from the perspective of a domain name holder. The purpose of this section of the Regulation is to ensure customers' actual access to information. In addition, FICORA would publish the prohibitive decision on its website.

7 Section 7 Obligation of the domain name registrar to advise holders

Section 7 of the Regulation lays down further provisions concerning how a domain name registrar must meet its obligation under section 170(1)(1) of the Information Society Code to inform and advise its customers. Under the provision, before registering a domain name, a domain name registrar shall provide information referred to in the Information Society Code on the requirements related to the content and form of a domain name. Section 7 of the Regulation lays down further provisions on the statutory necessary information to be provided to holders.

Pursuant to section 7 of the Regulation, before registering a domain name, a domain name registrar must provide holders with the following detailed information, in addition to what has been provided for in requirements concerning the content and form of the domain name in section 3(21) and section 166 of the Information Society Code:

1) requirements concerning the form of the domain name provided for in section 12 of the Regulation;
2) information on the names that have been entered into the Finnish Trade Register or into the registers of associations, foundations or political parties;
3) information on trademarks entered into the Finnish register of trademarks or the trademark register of the European Union.

The obligation of a domain name registrar to notify and advise has been explained in more detail in the preparatory material related to section 170(1)(1) of the Information Society Code. A domain name registrar should provide its customers and those who are seeking domain name registrations with the information referred to in section 166 of the Information Society Code in detail and without unnecessary trouble before registering a domain name. The information should be available to enable any applicants to confirm the requirements concerning the form and content of domain names before registering a domain name. In particular, customers should be aware of requirements concerning protected names

and trademarks before they register a domain name. The purpose of this provision is to help in avoiding incorrect and illegal domain name registrations, and a domain name registrar should, for its part, actively contribute to ensuring that domain name registrations comply with the law. The preparatory material related to this provision explicitly states that a domain name holder would still have the ultimate responsibility for the compliance of a domain name.

Pursuant to section 166(1) of the Information Society Code, a domain name shall include at least two but no more than 63 characters. Pursuant to subsection 2(1) of the provision, at the time of registration, a domain name shall not be based on a protected name or trademark owned by another party, unless the domain name holder can present a good, acceptable reason for registering the domain name. Under subsection 2(2) of the provision, at the time of registration, a domain name shall not be similar to a protected name or trademark owned by another party, if the clear intent of registering the domain name is to benefit from it or to cause damage.

Pursuant to the definition provided in section 3(1)(21) of the Information Society Code, a protected name or trademark means a name or trademark that has been entered into the trade register or into the registers of trademarks, associations, foundations, or political parties; or an established name, a secondary mark or trademark referred to in the Business Names Act (128/1979) or Trademarks Act (7/1964); or a name of a public body, unincorporated state enterprise, independent public corporation, public association, or diplomatic mission of a foreign State or its bodies.

Names entered into the trade register or into the registers of trademarks, associations, foundations, or political parties are listed in the registers of the Finnish Patent and Registration Office (PRH) and are publicly accessible through an online service maintained by the PRH. Trademarks that have been protected by registration in Finland are available either in the PRH's trademark database or in the register of the European Union Intellectual Property Office (EUIPO).

Pursuant to the definition in section 3(1)(21) of the Information Society Code, a protected name or trademark may also refer to an established name, a secondary mark or trademark referred to in the Business Names Act or Trademarks Act. Such unregistered names and trademarks are not available through the above registers. In its resolving practice, FICORA has taken a conservative approach to cancellation claims based on alleged establishment of a business name or a trademark before the registration of a disputed domain name. Dispute settlement by FICORA is an administrative process, and the evaluation of extensive evidence based on law relating to trademarks is not possible. Disputes concerning trademark law must be settled in a court, while FICORA may address obvious cases of trademark rights violations.

Section 7 of the Regulation refers to the requirements concerning the form of the domain name provided for in section 12. Such requirements include the definition of permitted characters for a domain name (the letters a to z and the numbers 0 to 9). In addition, the national characters listed in the Regulation and the hyphen-minus character are allowed. Section 12(2) of the Regulation also contains provisions concerning other technical details related to the form of domain names.

FICORA does not determine how a domain name registrar should meet its statutory obligation to provide information on the necessary items listed above. To meet the obligation, a domain name registrar could, for example, provide a link on its website that directs to up-to-date information as defined by FICORA. On its website, FICORA maintains up-to-date information on the statutory necessary information for end users and other helpful guidelines, such as information on FICORA's dispute-settling operations.

The preparatory material for the Information Society Code emphasises the responsibilities and obligations of domain name registrars when a new model in which domain name registrars assume an important role is being adopted. The preparatory material focuses on safeguarding the rights of domain name holders and an appropriate registering of domain names in the domain name register. For this reason, FICORA is of the opinion that under the Information Society Code, domain name registrars are obliged to advise their customers carefully.

8 Section 8 Holder-specific information to be entered in the domain name register

Section 8 of the Regulation lays down further provisions on the identifying information of a holder that a domain name registrar must enter in the domain name register when registering the domain name. For natural persons, the identifying and contact information provided for in subsection 1 of the section are the first and last name of the holder, as well as the address and telephone number necessary for reaching the holder. The identifying information of a natural person to be entered in the register also means a personal identity code or, if no personal identity code exists, other identifying information. Since foreign natural persons do not necessarily have a Finnish personal identity code, the other identifying information means a birth date.

Section 8(2) of the Regulation provides that the identifying and contact information of a legal entity or other community shall mean the holder's business name and the address and telephone number necessary for reaching the holder. The identifying information of legal entities to be entered in the register means the Finnish business identification number or, if no business identification number exists, other identifying information, such as other registration number. For legal entities, the Regulation also provides that the name, telephone number and email address of the holder's contact person must be entered in the register.

Pursuant to section 167(1) of the Information Society Code, a domain name shall be registered in the domain name holder's name. According to the preparatory material of the provision, the domain name belonging to a holder should not be registered in the domain name registrar's name or in any other name. The correctness of the registration of the holder is important for the exercise of the rights of the body that effectively holds the domain name, particularly if FICORA is settling a dispute or investigating an unclear issue under the Information Society Code.

Section 8 of the Regulation refers to a provision of the Information Society Code that obliges a domain name registrar to enter in the domain name register an email address for hearings and service of notices referred to in section 167 of the Information Society Code. Section 312(2) provides for FICORA's unconditional right to use the email address entered in the domain name register for hearings and service of notices, which means that documents or decisions related to domain names may always be issued by email. This "address for service" has major legal importance, and its notification is, under section 167 of the Information Society Code, mandatory for the domain name registrar. The use of address for service enables FICORA to quickly issue its binding decisions, since pursuant to section 312(2) of the Information Society Code, a decision or other document is deemed to have been received the third day after the sending of the message, unless provided otherwise. The correctness of a domain name holder's address for service is important information, and it is very important for the legal protection of the holder to keep it up to date.

The Information Society Code provides for the mandatory registration of only one email address, but the Information Society Code or the Regulation do not prevent the notification of email addresses other than those intended for official hearings or notices. It is possible to notify other email addresses to FICORA's online system, if the domain name registrar considers it necessary to keep email addresses intended for processing everyday technical issues related to the domain name separate from the mandatory address for service. Pursuant to section 167 of the Information Society Code, the domain name registrar shall enter in the domain name register the domain name holder's up-to-date information. According to the preparatory material related to this provision, notifying and maintaining correct information would be the responsibility of the domain name registrar. If the domain name holder suffered damage due to the negligence of the registrar, the holder should claim compensation in court. FICORA recommends that a domain name registrar informs FICORA without delay of any changes in the holder's information.

FICORA notes that the Personal Data Act (523/1999) is a general law on processing of personal data. Provisions of the Act apply to all processing of personal data unless other acts contain corresponding specific provisions. The Personal Data Act also brought into force the Data Protection Directive of the European Union. Several acts on different subjects also contain specific provisions on processing of personal data. They may concern, for

instance, the right to collect and record personal data, the right to disclose or store personal data, or the contents of a personal data file. Regulations of the European Union may also contain provisions that are directly applicable to the processing of personal data or that affect such processing. The Act on the Openness of Government Activities (621/1999) applies to disclosing of personal data from a personal data filing system controlled by an authority, unless otherwise provided for a specific function. Processing of personal data is also subject to provisions on secrecy and the principles of good information management. The Data Protection Ombudsman steers and supervises the enforcement of personal data legislation. More information about personal data regulation and the data protection reform to be completed in 2018 is available on the website of the Data Protection Ombudsman at www.tietosuoja.fi.

FICORA notes that all registrars of domain names that end with *fi* or *ax* are obliged to comply with personal data legislation, as applicable, in the processing of personal data. FICORA also states that it is an administrative authority that is subject to other regulation on Government activities such as the Administrative Procedure Act (434/2003). The Act on the Openness of Government Activities applies to disclosing of personal data from FICORA's domain name register. Publishing information on the domain name register on FICORA's internet pages is regulated in section 167(2) of the Information Society Code. The provision states that the domain name and the holder's name of natural persons may be published on the internet pages.

9 Section 9 Domain name registrar's interface to the domain name register of the authority in charge of domain names

Section 9 of the Regulation lays down provisions on the technical implementation of domain name register entries. Under subsection 1 of this section, a domain name registrar must use as the technical interface to the domain name register of FICORA either the browser-based user interface provided on the website of FICORA at www.ficora.fi or an EPP (Extensible Provisioning Protocol) interface defined and maintained by FICORA.

EPP is an XML-based technical interface defined in RFC documentation to which a domain name registrar can connect with its own client software. Because FICORA does not provide the client software, it is up to the domain name registrar to program or purchase the software. The EPP interface is not mandatory, but rather an alternative method used to make entries in the register and manage domain names instead of a browser interface. It is also possible for a domain name registrar to use both interfaces.

Under section 9(2) of the Regulation, if the domain name registrar uses the EPP interface determined by FICORA, the client software of the domain name registrar must be compatible with FICORA's EPP interface. FICORA's EPP interface is based on several RFC documents and follows their specifications as far as possible. The RFC documents have been listed in the References [8–15].

A description of the interface is annexed to Regulation 68 and the Regulation obliges domain name registrars to implement their EPP interfaces as described in the annex. Pursuant to the Regulation, the compliance must be verified with the EPP test system provided by FICORA. Testing the operability of a domain name registrar's EPP client software is a prerequisite for a registrar to begin using the software. The EPP client software must pass tests required by FICORA in an EPP test environment before the domain name registrar can start to use FICORA's EPP interface.

Section 9(3) of the Regulation contains requirements concerning the technical implementation of registration and management of domain names that end with *ax*. The provision lays down that a domain name registrar must use the browser-based user interface provided at www.whois.ax as the technical interface. This is a technical interface provided by the Government of Åland for domain name registrars registering and managing domain names that end with *ax*.

If the Government of Åland decides later to introduce an EPP interface of its own, the Regulation may be supplemented on the technical interface definitions concerning the registration and management of domain names that end with *ax*.

Pursuant to section 170(1)(3) of the Information Society Code, a domain name registrar shall be able to enter data in the domain name register using the technical systems prescribed by FICORA. According to the preparatory material related to the provision, a domain name registrar should have technical possibilities to make domain name registrations and perform other actions. The existence of technical possibilities is crucial for practical operations, because the domain name registrar would take care of all measures related to a domain name on behalf of the domain name holder.

10 Section 10 Transfer of a domain name to another holder

Section 10 of the Regulation defines a procedure to be followed when a domain name holder wishes to transfer the domain name to another holder. The registered holder of the domain name must request the transfer from the domain name registrar. After having received a transfer request, the domain name registrar must ensure that the holder has the right to transfer the domain name and request the authority in charge of domain names to submit a domain holder transfer key to the holder.

According to the new model, the domain name registrar is responsible for the technical implementation of the transfer. The register must take proper and adequate care to ensure that none other than the party registered as the domain name holder is requesting the transfer. The obligation to verify the holder's right to request a transfer is justified to ensure that the domain name registrar takes care in implementing this measure, which is relevant for the legal protection of the holder. If another natural person than the registered holder requests the transfer, the domain name registrar

must require proper authorisation from the holder. When the registered holder requesting the transfer is a legal entity, the registrar must confirm that the party that requested the transfer has the right to act on behalf of the holder. A confirmation means that the registrar requests further information, if the information provided with the transfer request does not match with the information held by the registrar or if the registrar has another reason to suspect that, for example, the holder has never given its consent to the transfer.

After verifying the holder's right to make a transfer request, a domain name registrar must request the authority in charge of domain names to submit the domain holder transfer key to the holder. The definition of a domain holder transfer key is included in section 3(1) of the Regulation. According to the definition, a domain holder transfer key means a code defined by the authority in charge of domain names that enables the transfer of a domain name from one holder to another. Therefore, the domain name registrar is not able to create the code. The purpose of this procedure is to ensure that the registrar cannot transfer a domain name to another holder without the holder's request. The authority in charge of domain names submits the domain holder transfer key to the holder, which can then forward it to the registrar for the purpose of transferring the domain name. The purpose of this procedure is to ensure the existence of an explicit intent by the domain name holder when a domain name is being transferred to another holder.

10.1 Domain name transfer time

Pursuant to section 10(2) of the Regulation, the domain name registrar must transfer the domain name to the new holder within five working days of the domain name holder submitting the domain holder transfer key and the details of the new holder to the domain name registrar. Such a reaction time may be considered a reasonable service level requirement, even if there are no obstacles to acting more quickly. Pursuant to section 168(1) of the Information Society Code, a domain name registrar shall transfer the domain name within reasonable time from receiving the request.

10.2 The role of the authority in charge of domain names in the process of transferring a domain name

If the transfer of a domain name does not take place within reasonable time, the authority in charge of domain names may take care of the transfer. In practice, for example FICORA would send the domain name transfer key to the holder at the holder's request. The intention is that the authority in charge of domain names adopts a secondary role when the new registrar model is implemented pursuant to the Information Society Code. However, it is necessary to ensure the possibility to transfer domain names in situations where the domain name registrar does not, for some reason, take care of its statutory obligations.

FICORA is responsible for ensuring compliance with law with regard to the code fi, and it may intervene in the operations of a domain name registrar,

if deemed necessary. In its controlling operations, FICORA may take action provided for in section 171(2) of the Information Society Code. If a domain name registrar violates the Information Society Code or rules, regulations or decisions issued by virtue of it, FICORA may issue the domain name registrar a note, a binding decision or, ultimately, a prohibitive decision. In the latter case, the registrar is forbidden from entering domain names or changes related to them in the domain name register for a maximum period of one year. In accordance with the present practice, the supervisory authority for the code ax is the Provincial Government of Åland.

10.3 The impact of a pending domain name dispute to the transfer procedure

Pursuant to section 168(1) of the Information Society Code, a domain name cannot be transferred if a case concerning the termination of a domain name has become pending before FICORA. The reason for this is that the processing of an unfinished dispute requires a decision to be made that concerns the parties, which is not possible if the parties could change during the procedure. When a dispute becomes pending, FICORA freezes a domain name, making it impossible to transfer. Freezing of a domain name does not otherwise affect the use of the domain name, which means that for example services related to the domain name, such as websites, can function normally.

10.4 Return of a domain name

Pursuant to section 168(2) of the Information Society Code, FICORA may return a domain name to its original holder if the domain name was transferred without the holder's consent and the holder requests a correction of the entry, and the recipient of the transfer does not present an acceptable reason for the transfer within a set period. According to the preparatory material for the provision, this provision would protect a domain name holder from intentional or unintentional incorrect transfers. The possibility of FICORA to correct a domain name transfer made in bad faith requires, according to the preparatory material for the provision, strong evidence of the fact that the domain name was transferred without the original holder's consent. Domain name registrars should ensure the adequate documentation of their transfer processes in order to make it possible to establish the course of events afterwards and to safeguard the legal protection of the domain name holder.

11 Section 11 Switch of domain name registrars

Section 11 of the Regulation defines a procedure to be followed when a domain name holder wishes to switch domain name registrars. As a rule, a domain name holder has two alternatives. The holder may contact directly the selected new registrar and request it to obtain the registrar transfer key from the old registrar. Alternatively, the holder may contact its contract partner, i.e. the old registrar, request the registrar transfer key and submit it to the new registrar. This means that the new registrar receives the

registrar transfer key either from the old registrar or from the holder, after which the new registrar can take control of the domain name.

The definition of a registrar transfer key is included in section 3(2) of the Regulation. Pursuant to the definition, a registrar transfer key means a code that enables the administration of a domain name to be transferred from one domain name registrar to another. As a rule, the code is created by the old registrar. The concepts of an old domain name registrar and a new domain name registrar have also been defined in subsections 3 and 4 of the section. An old domain name registrar means the registrar relinquishing the administration of a domain name when a domain is transferred from one registrar to another and a new domain name registrar means the registrar assuming the administration of a domain name when a domain is transferred from one registrar to another.

This provision of the Regulation requires that the domain name registrar ensures that the holder or the new domain name registrar has the right to request the registrar transfer key. In practice, the old registrar is expected to take proper and adequate care to ensure that none other than the registered domain name holder requests the registrar transfer. If the request is made by someone else, an appropriate authorisation to make such a judicial act must be presented. The domain name registrar may, for example, contact the holder to confirm that the authorisation indeed exists.

11.1 Registrar switch time and written request

Section 11(2) of the Regulation provides that the old registrar must submit the registrar transfer key to the requesting party within five days of a legitimate request. If the old registrar does not submit the registrar transfer key to the new registrar or holder within the specified time, the new domain name registrar may request that the authority in charge of domain names submits the registrar transfer key to the holder.

Pursuant to the preparatory material of section 168(3) of the Information Society Code concerning the switch of registrars, after the domain name holder has made its domain name registrar aware of its intention to switch domain name registrars, the registrar should take the measures that such a switch requires within a reasonable time and to contribute to a successful switching of domain name registrars. FICORA's Regulation defines that a reasonable time means five working days, but there is no obstacle for providing the service more quickly. If the domain name were not transferred to be managed by the new registrar within a reasonable time, the authority in charge of domain names could take care of the transfer. In practice, for example FICORA would send the registrar transfer key to the holder.

Section 11 of the Regulation requires that the request to switch domain name registrars must be made in writing – by email, for example. In this way, it is possible to determine afterwards when the deadline was or to clarify other confusions during the procedure.

11.2 The role of the authority in charge of domain names in the process of switching registrars

The Information Society Code provides for FICORA's role of being the ultimate alternative in situations where, for some reason, the old registrar fails to take care of its statutory obligations. The role of FICORA is to ensure compliance with law with regard to the code fi, and it may intervene in the operations of a domain name registrar, if deemed necessary. In its controlling operations, FICORA may take action provided for in section 171(2) of the Information Society Code. If a domain name registrar violates the Information Society Code or rules, regulations or decisions issued by virtue of it, FICORA may issue the domain name registrar a note, a binding decision or, ultimately, a prohibitive decision. In the latter case, the registrar is forbidden from entering domain names or changes related to them in the domain name register for a maximum period of one year. In accordance with the present practice, the supervisory authority for the code ax is the Provincial Government of Åland.

Pursuant to the preparatory materials for section 168(3) of the Information Society Code on switching domain name registrars, a domain name holder should be free to switch domain name registrars any time. No special reason should be required for switching a domain name registrar. The section should not lay down provisions on the contractual relationship between the domain name holder and the domain name registrar, and contract or consumer law issues arising from the transfer would be resolved under other legislation. It is stated in the preparatory materials for section 171 of the Information Society Code that FICORA's powers would not extend to settling contractual disputes between domain name holders and domain name registrars. Under section 303(2) of the Information Society Code, FICORA's decision-making power does not extend to agreement terms or compensation obligations between operators and subscribers. Agreements between operators and consumers are subject to the Consumer Protection Act (38/1978) which contains provisions, for instance, on contract terms, marketing of services and distance selling. The competent authority in consumer regulation is the Consumer Ombudsman whose most essential responsibility is to supervise that the Consumer Protection Act and other laws passed to protect consumers are observed. The Consumer Ombudsman does not primarily resolve individual disputes. These cases are handled by consumer rights advisors and the Consumer Disputes Board. More information about consumer protection is available on the website of the Finnish Competition and Consumer Authority at www.kkv.fi.

Chapter 3 Requirements concerning a domain name

This chapter explains the obligations of Chapter 3 of the Regulation, i.e. technical requirements concerning domain names.

12 Section 12 Domain name form

Section 12(1) of the Regulation lays down provisions on the permitted characters for a domain name, i.e. the letters a to z, the numbers 0 to 9 and the hyphen-minus character.

Subsection 2 of the Regulation includes a table of mainly such characters that separate the Swedish, Finnish and Sami alphabet from the Latin alphabet. Pursuant to the Regulation, the national characters identified in the list are permitted.

Character	Unicode	Name
-	002D	Hyphen-minus
á	00E1	Latin small letter a with acute
â	00E2	Latin small letter a with circumflex
ä	00E4	Latin small letter o with diaeresis
å	00E5	Latin small letter a with ring above
č	010D	Latin small letter c with caron
đ	0111	Latin small letter d with stroke
ǥ	01E5	Latin small letter g with stroke
ǧ	01E7	Latin small letter g with caron
ǩ	01E9	Latin small letter k with caron
ŋ	014B	Latin small letter eng
õ	00F5	Latin small letter o with tilde
ö	00F6	Latin small letter o with diaeresis
š	0161	Latin small letter s with caron
ŧ	0167	Latin small letter t with stroke
ž	017E	Latin small letter z with caron
ʒ	0292	Latin small letter ezh
ǯ	01EF	Latin small letter ezh with caron

In this table, the hyphen-minus has been identified with its Unicode symbol. Pursuant to section 12 of the Regulation, a domain name must not begin or end with a hyphen-minus. This is based on RFC document 1035 [3]. In addition, it is provided that a domain name must not begin with the characters xn--. The reason for this is that these characters have been reserved as the prefix of an ACE format internationalized domain name (IDN) containing national characters. Pursuant to section 12 of the Regulation, the ACE format (ASCII Compatible Encoding) of a domain name containing national characters always begins with the characters xn--. The requirements are based on the RFC documents RFC 3492 [4] and RFC 3490 [5].

Section 166(1) of the Information Society Code provides that a domain name shall include at least two but no more than 63 characters. This restriction follows the document RFC 1034 [6].

13 Section 13 Name servers

Section 13 of the Regulation deals with the configuration of name servers for domain names. The requirement only concerns domain names for which name servers have been entered in the domain name register. Name server configurations are not mandatory for a domain name. The name servers must be removed from the domain name register, if the domain name holder wants to keep a domain name in reserve without any associated functionalities, such as an email or a website.

At least two name servers that are independent of one another must be configured to serve the domain name. This helps to ensure the functioning of a domain name in case of a failure of one of the name servers. The maximum number of name servers determined by FICORA is ten. Name servers are independent of each other if they have different server devices and different IP addresses and have separate internet connections.

It must be possible to reach all name servers through the internet. It must also be possible to verify the name server configurations by name server requests made by FICORA. FICORA must verify the operation of all name servers. If one or more name servers are out of operation or the name server configurations are not correct, FICORA must send a note of this by email to the domain name registrar or to the email address of the name server administrator indicated by the domain name registrar.

Pursuant to section 13 of the Regulation, the name servers must be equipped with NS records (Name Server) that define all name servers of the domain name. The NS records must point to servers, for which an A record or an AAAA record (IP Address) or both have been configured in name service. The NS records may only be name servers that have actually been configured to serve the domain name. The NS records must be consistent with the information configured in the root fi.

Pursuant to section 13 of the Regulation, the SOA record (Start of Authority) that defines the configuration of the name server of the domain name must comply with the following:

1) the MNAME (Master Name) field must contain the name of the primary name server of the domain name;

2) the RNAME (Responsible Name) field must contain a working email address that belongs to the administrator of the name servers. The email address must be configured without the @ symbol, which is replaced by a dot; for example, hostmaster.domain.fi. The best practice is to configure the hostmaster address in the RNAME field in accordance with RFC 2142 [7].

FICORA recommends that the serial numbers and timers of SOA records should not differ essentially from published internet standards and recommendations. FICORA recommends the following:

```
example.com.  3600  SOA  dns.example.com. hostmaster.example.com. (
                         1999022301   ; serial YYYYMMDDnn
                         86400        ; refresh (  24 hours)
                         7200         ; retry   (   2 hours)
                         3600000      ; expire  (1000 hours)
                         172800 )     ; minimum (   2 days)
```

The recommended form of the serial number is YYYYMMDDnn, where YYYY is the year, MM is the month, DD is the day and nn is a running number that increases by one at each update. The number of the first version of the day is 01. The serial number helps to verify that the zone records of all domain name servers are the same. The serial number must not be zero (0).

The refresh and retry values determine how often secondary name servers check whether the domain name server information on the primary name server has been changed. The retry value determines the time of a new attempt to retrieve the name server information if the previous attempt was unsuccessful.

The expire value indicates how long the name server keeps the old zone record if a new record cannot be retrieved.

The minimum TTL value (time to live) determines the default lifetime of RRs (resource records). In some cases, it is justifiable to set the TTL below the recommended value; an example of such a case is a situation when there are changes to a name server.

FICORA's recommendations:

FICORA recommends that third parties are prevented from transferring domain name information (AXFR, DNS zone transfer protocol).

In addition, FICORA recommends that name servers should not return a correct value if the software version is inquired. If the correct software version is returned, information security may be compromised in cases where the name server software version has a known information security issue.

Chapter 4 Information security management by a domain name registrar

This chapter explains the information security requirements of domain name registering operations set out in Chapter 4 of the Regulation. The requirements of the Chapter are based on section 170(1)(6) of the Information Society Code, which provides that a domain name registrar shall ensure the information security of its operations. According to the

preparatory material of the provision, a domain name registrar should prepare detailed and adequate instructions for dealing with information security threats. A domain name registrar should ensure that events that are relevant for information security will not go unnoticed. In addition, a domain name registrar must address problems and irregularities identified in information security.

Pursuant to section 3(1)(28) of the Information Society Code, *information security* means the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data and information systems can be used by those who are entitled to use them. In other words, information security covers the measures taken to safeguard confidentiality, integrity and availability of information.

The Regulation describes the minimum requirements for managing information security that all domain name registrars should meet. The purpose of the requirements is to safeguard a basic level of information security in the registration operations of the domain name registrar, serving as a basis for ensuring the information security of the services provided. A particular focus of the requirements is on the continuous development, coordination, implementation and evaluation of information security management. Another purpose of the Regulation is to minimise the harmful impact of information security risks on the registration operations of domain name registrars and on the domain name holders.

14 Section 14 Consideration of information security issues

Information security is an essential element of the quality of the registration operations of a domain name registrar. The consideration of the various areas of information security is important in all stages of the service lifecycle: in coordinating, implementing and maintaining the service as well as in terminating the service. To make the consideration of information security an everyday routine, it is justifiable for a domain name registrar to establish the processes and practices that it will follow in the implementation of information security measures.

The domain name registrar must have documented procedures for ensuring information security. Up-to-date documents lay the foundation for systematic development and management of information security and help in the allocation of information security investments. The documentation also helps FICORA to verify, where appropriate, that the domain name registrar meets its obligations in terms of safeguarding information security.

14.1 Areas to be considered

Information security measures and the documents that describe the measures must take several matters into consideration. The section lists the themes that must be taken into account but does not establish specific requirements of how the different themes should be considered, since

appropriate information security measures may vary from company to company depending on such matters as the services offered. Minimum requirements concerning many of the themes listed in this section have been dealt with elsewhere in the Regulation. In terms of section 14 of the Regulation, the essential requirement is that the domain name registrar must identify the requirements that are relevant for its operations and the practices that best serve their implementation.

Examples of the aspects of information security management relevant to each theme are listed in the following. The list also contains references to the minimum requirements set by FICORA.

1. Administrative information security
   - Information security guidance documents (typical examples include information security policy and architecture) with which the management of the organisation proves its determination to ensure information security, the general principles of information security and its commitment to information security matters
   - Processes and their management
   - Management of risks and business continuity (see section 15 of the Regulation)
   - Documentation practices and systems
   - Auditing and rehearsing procedures

2. Personnel security
   - Personnel's information security responsibilities and obligations
   - Personnel's information security skills and skills development
   - Personnel's background investigations
   - Key employee risks
   - Prevention of risky combinations of responsibilities and tasks
   - Job rotation to detect irregularities
   - Procedures to be followed when employment is terminated
   - Misconduct and non-compliance of personnel

3. Security of hardware, software and data communications
   - Vulnerability management
   - Detection of information security violations (see sections 17 and 18 of the Regulation)
   - Change management (see section 19 of the Regulation)

4. Security of information material and usage
   - Safeguarding the confidentiality, integrity and availability of information
   - Classification of data and the treatment of data according to the classification (see section 16 of the Regulation)
   - Responsibilities related to the maintenance of a user right register: awarding, amending and cancelling user rights
   - Prevention of the accumulation of user rights
   - Prevention of unauthorised access to the administration and configuration data related to the provision of a domain name

registration service and to the invoicing, account and log data of the customers of the domain name registrar
- Data storage and deletion

5. Physical security
   - Location of facilities and the security of the surroundings
   - Access control
   - Structural protection

The Regulation requires that the above themes (1 to 5) are to be taken into account at the different stages of the lifecycle of a domain name registration service. This means that a domain name registrar must consider information security in coordinating, implementing and maintaining the service and in terminating the service.

14.2 Information security documentation

The Regulation requires a domain name registrar to have up-to-date documentation on the implementation of information security measures. As the Regulation does not specify the different documents that a domain name registrar must have, this is left to the discretion of the domain name registrar. What is essential here is that the documentation is updated and that it makes it possible to confirm that all the information security themes listed in the section have been considered.

15 Section 15 Risk management

A security risk refers to the likelihood of an injury or damage and its consequences. An information security risk means an accidental or deliberate event that compromises the confidentiality, integrity or availability of domain name registration operations. The difference between an information security risk and an information security threat is that the likelihood and consequences of a risk have been assessed.

Information security risks may arise from the following:
- human error;
- gaps in or non-compliance with the instructions provided to the personnel;
- theft or vandalism;
- flaws and malfunctions of equipment, systems or software;
- malware spread;
- destruction of data;
- damage due to fire or water;
- errors and neglect on the part of a subcontractor or a member of a partner network.

Risk management is a process that aims at identifying risks, reducing their likelihood and/or impact to an acceptable level and maintaining the achieved level. The purpose of risk management is to protect the organisation and its ability to perform its operations, taking into account economic factors.

The objective of risk management requirements is to ensure that a domain name registrar is aware of the consequences of the potential realisation of the risks and knows whether the risk-mitigating measures are adequate. The objectives of risk management include:

- speeding up recovery after information security problems;
- reducing the costs and damage caused by information security problems;
- helping in allocating investments that improve the information security of domain name registration operations;
- improving the quality and productivity of domain name registration operations;
- optimising, in terms of finances, the management of risks related to domain name registration operations;
- preventing the realisation of risks.

15.1 Identifying and addressing risks

Examples of standards and publications in which risk management has been discussed include the following: ISO/IEC 27005 [21], NIST 800-30 Risk Management Guide [22] and OCTAVE [23].

This Regulation does not set any obligation to follow a particular standard. Risk management models vary from company to company, and there is no single model that would suit every purpose.

The Regulation requires a domain name registrar to identify the risks related to its registration operations and its continuity and how to address them. Addressing the risks means that the domain name registrar determines an acceptable risk level to its operations and takes appropriate measures (often called controls) to reach this level. This means that practical risk management requires the determination of responsibilities and schedules. In addition, the implementation and impact of risk management measures should be monitored.

The Regulation also requires that the risk management is regular, i.e. that risks and the measures to manage them are evaluated on a regular basis. A domain name registrar is free to determine the appropriate monitoring cycles. Typically, risk assessment takes place in companies on an annual basis, whenever new services or functions are being established, and every time after a potential risk is realised.

15.2 Documentation of the process and its results

To enable the monitoring of compliance with the risk management requirements, a domain name registrar must document its established risk management process and results.

16 Section 16 Information material

In order to ensure that important information relevant to the domain name registering operations are only available to those who have the right to

access them, a domain name registrar must have in place a classification system and a processing procedure for the information material considered relevant for its registering operations.

16.1 Classification and processing of the material

A domain name registrar must determine a set of information material classification criteria that is appropriate for its own operations. An example of the classification of the materials is: public, confidential and secret.

In addition, a domain name registrar must determine how it processes (protects) the materials belonging to the different classes.

16.2 Information material documentation

The classification and the related processing instruction must be documented. Matters to be considered in the determination of the classification and its documentation include the following:

- general principles in assessing the security class and confidentiality of information material and in keeping the material secret;
- the rights to process and alter the materials and the distribution of the rights to access and alter the information material;
- determination of the confidentiality class;
- publicity of data or a document, including the right to speak publicly of the matter concerned;
- document properties: paper, watermark and other marks;
- storage and encryption;
- printing and copying;
- backup copies;
- sending and receiving, distributing and moving;
- documentation of the processing of the data and the document;
- document archiving, processing or the termination of processing rights, destruction of data and the document.

17 Section 17 Information security control

Section 17 of the Regulation contains further provisions on the domain name registrar's obligation laid down in section 170(1)(6) of the Information Society Code to ensure the information security of its operations. Some of these provisions are intended for information only. According to the preparatory material of the provision, a domain name registrar should ensure that events that are relevant for information security will not go unnoticed. If information security violations and threats related to domain name registration operations are to be detected, it means, in practice, that a domain name registrar must maintain a control mechanism of its services.

Proactive and prompt actions to detect various disturbances play an important role. If a domain name registrar is well equipped to identify disturbances, the measures to detect, control and remedy information security disturbances can be initiated quickly, without having to wait until

customers complain. The prevention of information security disturbances involves the detection of even the smallest signs of an emerging problem as early as possible. Through prevention, the impact on domain name registration operations can be minimised, and in best cases, there is no visible impact at all.

A domain name registrar must monitor constantly the state of information security in its domain name registration operations. A domain name registrar must have control mechanisms that are suitable for its registration operations and allow it to detect as quickly as possible any issues affecting information security. Examples of such situations include denial of service attacks, data leaks, hacking attempts and excessive user authorisations. A domain name registrar should also attempt to identify situations that are developing into problems as early as possible with its service management mechanisms. Data that help in predicting future disturbances include software alerts and service quality metrics that indicate deviations from normal operations even when an immediate disturbance is not detected. The determination of usable software alerts and quality metrics is the responsibility of the domain name registrar. Predictive information that helps in avoiding information security problems include alerts of detected hardware or software vulnerabilities.

The second subsection requires that the employed control mechanisms for domain name registering operations should be documented to allow, when necessary, the domain name registrar to prove how it meets the set requirements. Systems and procedures to be used for receiving and analysing various alerts and notifications must be documented and the documentation must be kept up to date. In other words, a domain name registrar must have a description of the technical systems and measures it uses to process information and alerts on the state of its services.

18 Section 18 Management of situations disturbing or threatening information security

Section 18 of the Regulation provides for the internal instructions of a domain name registrar concerning disturbances. The most important objective of the instructions is to provide the capability to find out the reason for an information security issue as quickly as possible and to minimise the impact of the event. The instructions also have practical importance in situations such as training of new personnel.

Pursuant to section 18(1) of the Regulation, a domain name registrar must prepare in advance and maintain a well-defined procedure for addressing situations that disturb or threaten the information security of registration operations and for minimising their impact and removing them without undue delay.

Pursuant to section 18(2) of the Regulation, the procedure must include at least the following:

- a description of the organisation of information security management;

- definitions of responsibilities, containing at least the information necessary for reaching the persons managing information security.

As a matter of course, the instructions should also take into account any special instructions concerning the corrective measures in case of major disturbances. Such special instructions may concern, for example, on-call or deputy arrangements.

Typically, the organisation of information security management is described in a company's internal information security policy, a set of documents describing the measures and targets of information security that has been approved by the company management.

19 Section 19 Change management

Section 19 of the Regulation provides that a domain name registrar must carry out changes to the network, software, hardware, configuration, interface and equipment facilities in a controlled and systematic manner so as to cause the least possible disturbance to the domain name registering operations. Pursuant to subsection 2, sufficient time must be reserved for carrying out changes, maintenance and updates to allow a controlled manner of executing a planned operation. In addition, pursuant to subsection 3, a domain name registrar must define and document the processes and practices guiding the changes.

The section acknowledges the principle that disturbances arising from changes, such as downtime, should be minimised. As downtime may sometimes be unavoidable and it should be possible to carry out planned alterations with as few errors as possible, the section emphasises the fact that in estimating the required downtime, not only the service needs but also the realistic time needed for carrying out the alteration carefully should be considered. Therefore, subsection 2 of the section explicitly provides for a "maintenance window" by requiring that sufficient time should be reserved for all measures.

To control change situations and to minimise damage, before starting the actual alteration work a domain name registrar must plan carefully the phases of the work and the required resources, estimate the impact and length of work, and plan in advance the measures to be taken if the work does not turn out as planned. For example, when the software of a device is replaced with another or its configuration is altered, it may be a good idea to simulate the impact of such alterations in advance as far as possible to allow for the detection and fixing of errors before they materialise.

A domain name registrar must establish and document the guiding processes and practices related to alteration work to enable a systematic and predictable approach to every alteration job.

For each alteration, maintenance or update measure, a domain name registrar must, on a case-by-case basis and according to its established

processes and practices, estimate and reserve adequate time for completing the alteration, maintenance or update job.

20 Section 20 § Katakri requirements in the use of FICORA's EPP interface

Section 20 of the Regulation describes the requirements that a registrar of domain names that end with *fi* must meet if it uses FICORA's EPP interface as its technical interface. In this case, the domain name registrar must meet the criteria derived from the requirements of the protection level (IV) of subdivision I, technical information security, of the currently valid version of Katakri with respect to the following:

1) Data Communications Security;
2) Security of Information Systems.

Katakri is the authorities' auditing tool, which an authority can use in assessing the target organisation's ability to protect an authority's classified information. The minimum requirements based on national legislation and international obligations are gathered in Katakri. The use Katakri 2015 auditing tool has been approved by the cooperation group of National Security Authority (NSA) on 26 March 2015. The aim was to make Katakri more future-proof to avoid frequent reforms.

Katakri, as such, does not set any absolute requirements for information security; instead, the requirements collected in Katakri are based on the legislation in force and the international information security obligations binding on Finland. The requirements in Katakri are marked with a reference to ensure transparency.

The requirements presented in Katakri are divided into three subdivisions:

Subdivision (T) concerning security management aims to ensure that the organisation has the sufficient ability and capability for security management.

Subdivision (F) concerning physical security describes the security requirements for the physical environment of processing classified information.

Finally, subdivision (I) concerning technical information security describes the security requirements for the technical data processing environment. This subdivision is divided into three protection levels in accordance with the processed data (ST IV, ST III, ST II).

The Regulation requires that the domain name registrars using FICORA's EPP interface shall meet the requirements in the subdivision of technical information security in terms of data communications security and security

of information systems. The purpose of the Regulation is to ensure the high level of information security of the customers of domain name registrars.

FICORA also notes that the requirements of the Regulation apply specifically to domain name registration operations, which is stated in section 2 of the Regulation describing the scope of application. If the party engaged in domain name registration operations also carries out other operations, the Regulation does not apply to such operations.

FICORA's Regulation refers to the currently valid version of the criteria. The valid version of Katakri is available on the website of the Ministry of Defence at defmin.fi.

Chapter 5 Obligation to notify disturbances

This chapter explains the obligations laid down in Chapter 5 of the Regulation. The obligations referred to in this chapter specify the requirements laid down in section 170(1)(7) of the Information Society Code on the notifications to be made to the authority in charge of domain names on significant disturbances of information security.

21 Section 21 Disturbance notification by the domain name registrar to the authority in charge of domain names

Section 21 of the Regulation lays down further provisions on the content of a domain name registrar's notification obligation on disturbances of information security.

The obligation on domain name registrars laid down in section 170(1)(7) of the Information Society Code is a new addition. Under this section, a domain name registrar shall notify FICORA without undue delay of significant violations of information security in its domain name services and of anything that essentially prevents or disturbs such services. A domain name registrar shall also make a notification of the estimated duration and consequences of the disturbance or threats of such disturbances, and of measures undertaken to rectify the situation and prevent the reoccurrence of such violations. The preparatory material related to the provision provides an example of a situation where the system of the domain name registrar has been intruded. The supervising authority must be notified immediately, since there is a risk that the intruder may be able to freely alter the details of the domain names managed by the domain name registrar, such as name servers. The preparatory material related to the provision further acknowledges that the threat is limited to the customers of the domain name registrar, but the number of customers affected may be large. In accordance with the present practice, the supervising authority for the code ax is the Provincial Government of Åland and any related disturbance notifications should be submitted to it.

Pursuant to section 21(1) of the Regulation, in a notification concerning a significant disturbance of information security, a domain name registrar must, in addition to the information laid down in the Information Society Code, provide, where possible, information concerning the reason of the disturbance or threat and how it emerged. Pursuant to subsection 2, the disturbance notification must be made within 24 hours of the domain name registrar becoming aware of the disturbance. The notification must be supplemented later with the information that was not available at the time of making the notification.

21.1 Significant violations of information security

Pursuant to section 170(2) of the Information Society Code, FICORA may issue further regulations on whether a violation referred to in subsection 1(7) is significant and the content, form and delivery of a notification.

At this point, FICORA has not considered it necessary to provide further regulations to determine when a violation of information security is a significant one. It is possible to issue an amended Regulation at a later date to define the notification threshold more precisely, if this is found to be necessary in light of the supervision experience. Nevertheless, FICORA is of the opinion that it is necessary to highlight some aspects to be considered in the assessment of significance.

When assessing the significance of a violation of information security or another event, it is necessary to pay attention to the adverse effects of the event or the seriousness of the information security threat caused. Violations of information security may affect the confidentiality, integrity or availability of data or information systems.

Here, confidentiality means that the data and the authentication data related to user IDs are known only by authorised parties. Integrity means that it is not possible to alter the data without authorisation and that third parties are not able to tamper with information systems. Availability means that the service and the data contained are available to those who are authorised to access them.

The following should always be protected, and any information security disturbances in them are to be considered significant:

- services provided by the domain name registrar itself, as well as the information and communication systems employed in providing the services;
- information security, protection of personal data and business secrets of the customers of the domain name registrar;
- the Finnish fi root administered by FICORA following a violation of information security that directly or indirectly affects a domain name registrar.

Repeated, exceptionally lengthy or obviously deliberate action with a negative impact on a domain name registrar's ability to ensure the information security of its registration operations is also to be considered significant.

Similarly, a disturbance is to be considered significant, if it is not possible to eliminate it through action taken by the domain name registrar only.

21.2 Examples of violations of information security falling within the scope of notification obligation

The following list contains examples of violations of information security of which FICORA considers it necessary to make a notification referred to in section 170(1)(7) of the Information Society Code. The list is not exhaustive, and it is intended to clarify the severity level of the notification threshold. Significant disturbances of information security referred to in the above provision that should be notified include the following:

21.2.1 Hacking of the information systems of a domain name registrar

- Unauthorised access to the system of a domain name registrar
- Vulnerability or configuration error in the system of a domain name registrar that compromises information security

21.2.2 Accidental disclosure of logins to third parties

- Logins to FICORA's systems falling into the hands of third parties

21.2.3 Unauthorised alterations

- An opportunity to make unauthorised changes to domain names administered by a domain name registrar
- Unauthorised changes made by the staff of the domain name registrar to FICORA's domain name registry
- Unauthorised access to the self-service portal provided by the domain name registrar to its customers, intended for enabling customers to maintain the information related to their domain names

21.2.4 DoS attacks

- If the system of the domain name registrar is paralysed and/or customer access to the system is prevented
- The system failure affects the operation of FICORA's system

21.3 Recommendation on voluntary notifications

FICORA recommends that at their discretion, domain name registrars notify FICORA also violations of information security that are not significant and the threats of such violations. Such knowledge may be relevant in undertaking the measures referred to in section 172 of the Information Society Code or from the perspective of FICORA's other information

security duties laid down in section 304, subsections 1(1), 1(7), 1(8) and 1(10).

Pursuant to section 172(1) of the Information Society Code, FICORA has the right to undertake the necessary measures in order to detect, prevent, investigate and commit to pre-trial investigation any significant information security violations aimed at public communications networks or services using .fi code domain names or their holders. FICORA may undertake these measures without consulting the domain name holder.

Pursuant to subsection 2, the necessary measures referred to in subsection 1 above may be actions targeted at root fi name server data and may include the following:
1) prevent and restrict traffic to the domain name;
2) reroute traffic to the domain name to another domain name address; and
3) any other comparable technical measures in the meaning of subsections 1–2.

Pursuant to subsection 3, any measures referred to in section 172 shall be implemented with care, and they shall be commensurate with the seriousness of the information security violation being combated. Such measures shall not limit freedom of speech, the confidentiality of a message or the protection of privacy any more than is necessary for the purpose of safeguarding the goals referred to in subsection 1. Such measures shall be discontinued if the conditions specified in this section for them no longer exist.

Section 304 of the Information Society Code lays down provisions on the special duties of FICORA. Under this provision, the duties of FICORA are:

- promote the functionality, freedom from interference and security of telecommunications (subsection 1);
- collect information on violations of and threats to information security in respect of network services, communications services and added value services as well as on defects and interference situations in communications networks and services (subsection 7);
- disseminate information security matters as well as communications network and service matters (subsection 8); and
- investigate violations of and threats to information security in respect of network services, communications services and added value services (subsection 10).

21.4 Notification procedure

The discovery of a disturbance relating to information security must be notified to the authority in charge of domain names as soon as possible, but within 24 hours at the latest pursuant to section 21(2) of the Regulation. The notification to FICORA shall be made primarily by email to the address cert@ficora.fi. If the disturbance of information security is

serious and/or the domain name registrar needs help in finding out the unauthorised changes, it is advisable to contact FICORA also by telephone.

If all information to be provided in the notification is not available (see 21.5 below) and the situation must be examined in more detail, a so-called preliminary notification must be made within 24 hours, which must then be complemented as soon as possible, but no later than three (3) days after the preliminary notification.

If, in spite of its investigations, the domain name registrar is not able to provide all information within three days of the preliminary notification, the information that has become available before this deadline must be notified, along with reasons why the rest of the information will be notified after the deadline.

The information already notified must be updated as necessary and as soon as possible when the information changes.

21.5 Information to be notified

The following information must be provided to the authority in the notification:

- Details of the domain name registrar, i.e.:
  - name of the domain name registrar
  - name, email address and telephone number of the person who provides additional information on the incident
- Date and time of the incident and when it was detected:
  - the date and time of the incident and the time when it was detected must be reported separately
  - if the exact time of the incident is not known, at least the date must be reported
  - the precise time of the technical system logs that indicate the event must also be reported, including the time zone (such as "UTC+2" and the potential offset of the clock and its direction compared to the official time
  - the time stamps of technical system logs should be reported in an ISO 8601 compatible format (cf. http://www.w3.org/TR/NOTE-datetime), but the most important thing is that at least some observation data is still available
- The type of the incident, i.e. whether the event concerns any of the following:
  - hacking or unauthorised access (such as break-in to an application connected to FICORA's EPP interface);
  - error in the management of customer data (such as an unintentional leakage of customer information); or

  - another event, in which case the incident must be described in words.

- A description of the affected system and the measures taken, i.e.:

  - a description of the system affected by the incident
  - observations on the progress of the events
  - details of the cause of the incident
  - measures already taken or that will be taken to eliminate or mitigate the impact
  - an indication of whether measures have been taken to prevent further damage

- Details of potential impact on users, i.e.:

  - a description of the potential impact
  - details of the domain names subjected to unauthorised editing
  - if the domain name registrar does not know what kind of unauthorised changes have been made to FICORA's systems with the domain name registrar's login, this must also be reported

Chapter 6 Provisions on entry into force

This chapter deals with the provisions of Chapter 6 of the Regulation, i.e. the provisions concerning the entry into force of the Regulation.

22 Section 22 Entry into force

The Regulation enters into force on 5 September 2016 and will remain in force until further notice.

23 Section 23 Information and publication

The Regulation is included in the Series of Regulations issued by the Finnish Communications Regulatory Authority and can be obtained from the FICORA Customer Service Office.

In addition, the Regulation and the accompanying memorandum on the explanations and application of the Regulation must be published online on FICORA's website and in Finlex, the Electronic Statutes of Finland (www.finlex.fi), under authority regulations.

PART C Other matters related to the subject matter of the Regulation

1 Recommendation of FICORA on the adoption of DNSSec

FICORA recommends that the domain name registrar promote the use of DNSSec technology in their domain name registration operations. DNSSec (Domain Name System Security Extensions) is a standardised security extension of the Internet Domain Name System. Its purpose is to improve the security and reliability of name service with digital signatures added in name service records.

The functionalities provided by DNSSec help in verifying the origin of the name service data and the integrity of the data, but DNSSec also makes it possible to verify the authenticity of negative responses. To implement the above functionalities, DNSSec specifies new record types in the name service. The main record types are RRSIG, DNSKEY, DS and NSEC(3). The functionalities of DNSSec are based on so-called chains of trust, in which the public keys of signed zones can be verified with the public key of a signed parent zone. In an ideal situation, the chains of trust begin from a signed root zone with a public key that has been pre-determined to be reliable. To ensure the overall reliability of a name service, it is crucial that every link of a chain of trust can be trusted.

DNSSec is not designed to replace TLS encryption (Transport Layer Security), but to complement it and prevent situations in which the user ends up in the wrong server even before the connection has been secured with TLS.

FICORA recommends that domain name registrars adopt DNSSec for all domain names they are managing or offer it for all their customers (domain name holders), if the domain name registrar has its own name servers.

More information on the DNSSec security extension can be found on FICORA's website at https://domain.fi.

PART D Legislation

1 Legal basis of the Regulation

FICORA's Regulation is based on the Information Society Code (917/2014). Provisions on domain names are mainly laid out in Chapter 21 of the Information Society Code. In addition, there are provisions concerning domain names in the following chapters:

- Chapter 1, section 3 (Definitions), subsections 21 and 35
- Chapter 36, section 295 (Domain name fee)
- Chapter 39, section 312 (Electronic notification)
- Chapter 43, section 343 (Appeals to the Market Court)

- Chapter 45, section 351 (Entry into force)

Chapter 21 of the Information Society Code lays down provisions on FICORA's authority to issue regulations:

Pursuant to section 165(3) of the Information Society Code, FICORA may issue further regulations on the notification and its content. Subsection 1 of the section lays down the domain name registrar's obligation to submit a notification when it launches its operations. Subsection 2 of the section lays down the obligation to notify any changes in the provided information, the termination of operations and a prohibition decision made by FICORA pursuant to section 171(2).

Pursuant to section 166(3) of the Information Society Code, FICORA may issue further regulations on specifications, form, length and permissible characters necessary for a functional domain name. Pursuant to subsection 1 of the section, a domain name shall include at least two but no more than 63 characters. Subsection 2 of the section provides for the form of a domain name.

Pursuant to section 167(4) of the Information Society Code, FICORA may issue further regulations on the technical implementation of registration and the information to be submitted. Pursuant to subsection 1 of the section, the domain name registrar shall enter in the domain name register the domain name holder's correct, up-to-date and identifying information as well as the email address to be used for hearing and service of notices.

Pursuant to section 168(4) of the Information Society Code, FICORA may issue further regulations on the technical implementation and time periods for transfers and switching domain name registrars. Pursuant to subsection 1 of the section, a domain name holder may transfer the domain name to another holder during its validity period. A domain name registrar shall transfer the domain name within reasonable time from receiving the request. Pursuant to subsection 2 of the section, a domain name holder may switch domain name registrars while a domain name is valid. The domain name registrar shall take the measures required to make this switch within a reasonable time from receiving the request.

Pursuant to section 170(2) of the Information Society Code, FICORA may issue further regulations on the information to be provided to a domain name holder, information security of operations, whether a violation referred to in subsection 1(7) is significant and the content, form and delivery of a notification. Pursuant to subsection 1(1) of the section, before registering a domain name, a domain name registrar shall provide information referred to in the Information Society Code on the requirements related to the content and form of a domain name. Pursuant to subsection 1(6), a domain name registrar shall ensure the information security of its operations. Pursuant to subsection 1(7), a domain name registrar shall notify FICORA without undue delay of significant violations of information security in its domain name services and of anything that essentially prevents or disturbs such services. Under the provision, a

domain name registrar shall also make a notification of the estimated duration and consequences of the disturbance or threats of such disturbances, and of measures undertaken to rectify the situation and prevent the reoccurrence of such violations.

Reference list

[1] Information Society Code [917/2014]; for an up-to-date version, see www.finlex.fi

[2] National Security Auditing Criteria (Kansallinen turvallisuusauditointikriteeristö Katakri):
1) Data Communications Security
2) Security of Information Systems,
www.defmin.fi

[3] IETF 1035 Domain names - implementation and specification: http://www.ietf.org/rfc/rfc1035.txt

[4] IETF RFC 3492 Punycode: A Bootstring Encoding of Unicode for Internationalized Domain Names in Applications (IDNA): http://www.ietf.org/rfc/rfc3492.txt

[5] IETF RFC 3490 Internationalizing Domain Names in Applications (IDNA): http://www.ietf.org/rfc/rfc3490.txt

[6] IETF RFC 1034 Domain names - concepts and facilities: http://www.ietf.org/rfc/rfc1034.txt

[7] IETF RFC 2142 Mailbox Names for Common Services, Roles and Functions: http://www.ietf.org/rfc/rfc2142.txt

RFC documents concerning FICORA's EPP interface:

[8] IETF RFC 3375 - Generic Registry-Registrar Protocol Requirements: https://www.ietf.org/rfc/rfc3375.txt

[9] IETF RFC 3735 - Guidelines for Extending EPP: https://tools.ietf.org/rfc/rfc3735.txt

[10] IETF RFC 5910 - Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP): https://tools.ietf.org/rfc/rfc5910.txt

[11] IETF RFC 5730 - Extensible Provisioning Protocol (EPP): https://tools.ietf.org/rfc/rfc5730.txt

[12] IETF RFC 5731 - Extensible Provisioning Protocol (EPP) Domain Name Mapping: https://tools.ietf.org/rfc/rfc5731.txt

[13] IETF RFC 5732 - Extensible Provisioning Protocol (EPP) Host Mapping: https://tools.ietf.org/rfc/rfc5732.txt

[14] IETF RFC 5733 - Extensible Provisioning Protocol (EPP) Contact Mapping: https://tools.ietf.org/rfc/rfc5733.txt

[15] IETF RFC 5734 - Extensible Provisioning Protocol (EPP) Transport over TCP: https://tools.ietf.org/rfc/rfc5734.txt

Other internet standards and recommendations related to the Regulation:

[16] IETF RFC 1912 Common DNS Operational and Configuration Errors: http://www.ietf.org/rfc/rfc1912.txt

[17] IETF RFC 2181Clarifications to the DNS Specification: http://www.ietf.org/rfc/rfc2181.txt

[18] RFC 2182 Selection and Operation of Secondary DNS Servers: http://www.ietf.org/rfc/rfc2182.txt

[19] RIPE 192 Simple DNS Configuration Example. RIPE DNS Working Group: http://www.ripe.net/ripe/docs/ripe-192.html

[20] RIPE 203 Recommendations for DNS SOA Values: http://www.ripe.net/ripe/docs/ripe-203.html

Risk management standards and publications related to the Regulation:

[21] ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management: http://www.iso.org/iso/home.htm

[22] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems: http://www.nist.gov/

[23] Software Engineering Institute (SEI) at Carnegie Mellon University, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): www.cert.org/octave/