# TABLE OF CONTENTS

**FOREWORD**  
4  

**INTRODUCTION**  
4  

**THE INTERNET ADDRESS SYSTEM**  
5  
Organization of the domain name system  
6  
What happens when a domain name is looked up?  
7  

**NORWEGIAN DOMAIN NAMES**  
8  
Legal framework  
8  
Organizations, roles and responsibilities  
8  

**WHEN A CONFLICT ARISES**  
9  
Domain name conflicts – measures  
10  
Conflicts concerning content or services – measures  
10  
  Removing the content or the service  
10  
  Deleting the domain name linked to the content or service  
10  
What happens when a domain name is deleted?  
11  

**WHAT CAN BE DONE THROUGH NORID’S SYSTEMS?**  
12  
Voluntary measures  
12  
Compulsory measures  
12  
  Compulsory measures in civil cases  
13  
  Compulsory measures in criminal cases  
13  

**CONTACT INFORMATION**  
15
FOREWORD

The world of the Internet generally and domain names specifically is currently undergoing an intense period of technical and political development, and over a very short period both factors have become important parts of the infrastructure of modern society. Not unexpectedly, conflicts around these issues arise, such as those linked to branding rights on the registration and use of domain names, combined with issues linked to investigational approaches and the processing by the courts of illegal activities carried out on the Internet. This guide about the Internet and domain names has been prepared to provide those involved such as judges, lawyers, prosecuting authorities and the police, with a level of knowledge of the technical and practical aspects of conflict resolution and the legal processes in this field.

The discipline is undergoing constant development so there will be a need to keep this information updated. For this reason we recommend that you bookmark our website (www.norid.no/index.en.html) where you will always be able to find the most recent version of this guide and other relevant information. We are of course always at your disposal if you wish to make a direct enquiry.

We hope that the guide will be a useful tool in your day-to-day work surrounding these issues, and we will be only too pleased to receive your suggestions as to how to develop the information to be even better.

Trondheim, January 2012
Hilde M. Thunem
Managing Director

INTRODUCTION

In this guide we explain what a domain name is, how the global domain name system is linked together, and how the Norwegian component of this system is organized. We describe the organizations involved, their roles and responsibilities, and explain the difference between a dispute involving the domain name itself, and a conflict about services or content found within a given domain.

Furthermore, we describe what happens when a domain name is deleted. It is important to be aware of the benefits achieved on deletion, but it is also important to be fully aware of what we fail to resolve when we delete a domain, and the unintended consequences that can result from a deletion.

In conclusion, we provide an overview of the operations that can be carried out on a Norwegian domain name, and how conflicts can be managed both within and outside the legal system.

ABOUT NORID

UNINETT Norid AS (Norid for short) operates the .no domain and maintains the central register for Norwegian domain names. We process applications, delegate new domains and are responsible for the regulations governing this important aspect of the modern society’s infrastructure. We are also responsible for .no’s names service, which ensures that Norwegian domains are globally accessible at all times. Norid is closely involved in collaborative international efforts in this field.

The company is part of the UNINETT Group, which is owned by the Norwegian Ministry of Education and Research. Our services are governed by special statutory regulations and are subject to the regulatory provisions of the Norwegian Post and Telecommunications Authority.
THE INTERNET ADDRESS SYSTEM

It is the services provided on the technical infrastructure that represent value to Internet users. The best-known services are websites and email, but it is also possible to use the net for activities such as connecting telephone conversations, downloading files and logging on to various databases.

So how do we get access to these services? All computers linked to the Internet have their own IP address, which consists of a long series of numbers. Using this address makes it possible to connect directly to a computer. However, to save users from having to remember long strings of numbers, the Domain Name System (DNS) attaches a unique domain name to the IP address in question.

The terms domain name and domain are used interchangeably.

The domain name system represents the Internet’s “telephone book”. The domain name is used to look up addresses in the domain name system in the same way as you look up a name in a telephone book in order to find the right number. This lookup process sets in motion a search for an IP address which is then used to contact the computer offering the service you require access to. We all know that a telephone conversation is not conducted through the telephone book itself. In the same way, Internet traffic does not pass through the domain name system.

Norwegian domain names are commonly written in the form companyname.no. If the domain name offers services such as websites and email, the web address may be www.companyname.no, and a typical email address within the domain may be written in the form firstname.surname@companyname.no.

It is important to note that it is possible to register and hold a domain without it offering services to users.

A domain name is always unique. Because their spelling is different, domain names such as regjeringen.no and regjeringa.no (Norwegian government websites) represent two different domains. This rule applies even if the two names share the same meaning and the same domain holder, and point to the same IP address.
ORGANIZATION OF THE DOMAIN NAME SYSTEM

The domain name system is structured as a hierarchy and can be compared with a plant’s root system. The uppermost level is often called the DNS root zone, or just the “root”. The so-called “top level domains” represent the uppermost level immediately below the root. There are two types of top level domains. The first are the country codes, such as .no (representing Norway) and .se (Sweden), and regulations governing these are drawn up at the national level. The second are the generic top level domains such as .com, .org and .net. Regulations governing these domains are stipulated at the global level.

Below the top level domains we find what we most commonly associate with the term “domain names”, (second-level domains) such as uio.no for the University of Oslo. Some top level domains also have their own so-called “second-level category domains” at this level. These domains are set up for specific groups, such as dep.no, which is a category encompassing all the Norwegian government ministries, or priv.no, which is a category used for private domain names. At the next level down we find the so-called “sub-domains” such as minestudier.uio.no, and the names of computers such as stream-prod02.uio.no.

The root structure also reflects the levels of responsibility linked to the domain name system. Separate organizations have responsibility for ”rootlets” at respective levels.

A variety of registries administer the regulations and operate the central database for each individual top level domain. Norid assumes this role for the Norwegian country code .no. A user who has registered a Norwegian domain name (the holder) is entitled to create whatever sub-domains he wants. Rights and obligations pursuant to the regulations governing the Norwegian top level domain rest at all times with the holder, regardless of whether he has given a third party permission to establish a sub-domain.

An individual person or organization can only influence the rootlet immediately below its own level in the hierarchy. This means that Norid cannot influence a domain such as .com or domain names registered within this top level domain.
WHAT HAPPENS WHEN A DOMAIN NAME IS LOOKED UP?

Each domain name is linked to a series of computers which respond to enquiries regarding addresses registered within the domain name. These computers are called name servers. For the most part, the user is unaware of communication with these computers.

An example of a typical enquiry:
You want to look up a specific event posted on the University of Oslo’s website. You know that the university’s address is www.uio.no, so you enter this in your browser’s address field.

1. A small software application in your computer contacts a separate computer – a so-called “recursive resolver” – which has been set up to process enquiries made to the domain name system. This computer is usually located on the premises of the Internet Service Provider (ISP).

2. The job of the recursive resolver is to find the IP address for www.uio.no. It sends the enquiry onwards to one of the name servers for the root in the domain name system. The root name servers recognize only the level below them in the hierarchy and so send back a list of the name servers for .no.

3. The resolver then re-sends the enquiry to one of the name servers for .no. These also recognize only the level immediately below them, and so send back a list of the name servers for uio.no.

4. The resolver repeats the enquiry to one of the name servers for uio.no, which responds with the IP address for www.uio.no.

5. The resolver then sends the IP address to your computer. When your browser receives the address, it can then contact the university’s web server and download the website you want.
NORWEGIAN DOMAIN NAMES

The term “Norwegian domain names” refers to those domain names registered within the Norwegian country code. All domain names listed directly within the country code are registered in our database. As of January 2012 there was a total of more than 540,000 registered names. Each month we process about 6,500 new domain name applications.

LEGAL FRAMEWORK

The Norwegian top level domain is administered in compliance with Norwegian legislation, cf. Section 7-1 of the Norwegian Electronic Communications Act, and the statutory regulations governing domain names (the Domain Regulation). The Domain Regulation sets out the terms of reference for the administration and formulation of, and amendments to, the policy governing the .no domain.

Section 7-1 of the Norwegian Electronic Communications Act:
www.lovdata.no/all/tl-20030704-083-007.html#7–1

The statutory regulations governing domain names:
www.lovdata.no/for/sf/sd/sd-20030801-0990.html

Process for the development of the policy governing the .no domain:
www.norid.no/regelverk/rammer/regelverksprosess.en.html

For several years, the Norwegian registration service has been fully automated in order to meet requirements related to such issues as cost effectiveness and predictability as stipulated in the Domain Regulation. This automation also meets the user’s need for swift processing of applications. Prior to registration, the applicant signs a self declaration in which he confirms that he is not infringing the rights of others and that he assumes full responsibility for the consequences of his registration and use of the domain name he selects. No prior checks are made by Norid to determine if a registration infringes the rights of others. Infringement of rights and other conflicts are thus handled retrospectively, either by the Alternative Dispute Resolution Committee or by legal proceedings.

ORGANIZATIONS, ROLES AND RESPONSIBILITIES

Three parties are involved in the registration of Norwegian domain names: The holder, the registrar and Norid itself.

The holder is the party intending to use a domain name on his own behalf. The registrar submits applications on behalf of the holder and acts as an intermediary between the holder and Norid. Norid processes applications in compliance with the regulations, completes the registration process in the central register, and operates the name server for .no.

The relationship between these three parties is governed by civil legal agreements. The domain name policy for .no acts both as a contract between Norid and the holders, and between Norid and the registrars. Norid also has a separate contract with the registrars. The figure on the following page illustrates the relationship between the three parties.

A party which applies for and is allocated a domain name then has a right to use the name for as long as the registration remains valid – normally until the time at which the holder decides to terminate it.
How to find the holder: Norid offers its own lookup service where you can find out who the holder is for a domain, and see what other domains the same holder has. As a supplementary service, we also maintain a list of registries for top level domains other than .no. This service is useful if you need to contact someone regarding a domain within other top level domains than .no.

How to find the service provider: Norid's lookup service provides information about which name servers host domains registered within .no, the name of the person responsible for technical matters, and the name of the registrar. Some of this information may point to the identity of the technical supplier of the services provided within the domain.

When a conflict arises

For services provided within domains and website content, Norwegian law applies in the normal way. The holder bears the full and sole liability for use of the domain. It is the holder who determines whether services shall be linked to the domain and which services he intends to offer. These may be services which he chooses to provide himself within his own organization and on his own computers, or he may purchase products offered by an ISP or other service providers. The services can vary in terms of content – from static websites to websites containing files for download, online games, portals such as altinn.no, and a wide variety of other services.

Two types of conflict involving domain names can arise: The first are those in which the domain name itself constitutes the focus of the dispute. The second are those in which the domain name is involved because it leads to content which becomes the subject of dispute. Under normal circumstances, Norid is not a party to these conflicts. Nor do we need to be in order to be able to take the necessary steps.

Conflicts regarding the domain name. For the most part, such conflicts concern civil law cases involving disputes over user rights to the domain in question. In theory it is also possible to imagine cases where one party argues that a domain name is in itself slanderous or illegal.

Conflicts regarding content and services. In the event of infringement of the law and unwanted activity on the Internet, it is usually the services and not the domain name which constitute the problem. Both websites and email may contain illegal content, or be used for illegal purposes such as attempts to commit fraud. Such conflicts often result in criminal proceedings in which the prosecuting authorities argue for the shutting down of a given content or service. It may also be the case that other parties, from either the private or public sector, may wish to shut down the content on a given website.
DOMAINT NAME CONFLICTS – MEASURES

Disputes concerning rights to domain names can be brought before the Alternative Dispute Resolution Committee (ADR Committee for short). The ADR Committee acts as a fast, economic and straightforward alternative in obvious cases of conflict. The Committee is empowered to determine both that a domain name shall be transferred and that it shall be deleted. In their contract with Norid, domain holders undertake to participate in the complaints process and to be bound by decision handed down by the Committee. Both parties are entitled to bring the dispute before the court at a later date (see page 13).

THE ALTERNATIVE DISPUTE RESOLUTION COMMITTEE

The ADR Committee is an impartial body which considers disputes concerning the rights to domain names and complaints made regarding decisions taken by Norid. In its role as a secretariat, Norid is responsible for preparing case documents, but makes no submissions in the cases themselves. All decisions of the Committee are published on both Norid’s and Lovdata’s websites. (Official webservice containing legal information (laws, regulations, court verdicts, etc.).)

The Alternative Dispute Resolution Committee:
www.norid.no/domenekonflikter/domeneklagenemnda/index.en.html
ADR archive:
www.norid.no/domenekonflikter/klagearkiv
(in Norwegian only)
Court decision archive:
www.norid.no/domenekonflikter/rettssaker
(in Norwegian only)

CONFLICTS CONCERNING CONTENT OR SERVICES – MEASURES

Removing the content or the service
The only effective means of making an illegal service entirely inaccessible without any negative impact on other parties, is to shut down the service. This can only be achieved locally on the computers on which the service is provided. This is the reason why the most effective approach in all cases is either to take steps focused directly against the domain holder or to contact the service provider.

Measures against the holder. The natural starting point in a conflict concerning content or services on the Internet is with the holder. Some conflicts are resolved by the holder voluntarily removing content or shutting down the disputed services.

NorSIS (Norwegian Centre for Information Security) offers advice and guidance through their service “delete me” to the public and others as to how best to proceed with such enquiries.

Advice and guidance through NorSIS and their service “delete me”:
www.slettmeg.no
Email hjelp@slettmeg.no
Phone +47 08247

If you are unsuccessful using this approach, legal proceedings represent an alternative means of instructing the holder to shut down the services in question.

Contact the service provider. If it is not possible to contact the holder, the next step is to contact the service provider. In many cases this will be the Internet Service Provider (ISP).

The majority of Norwegian ISPs have guidelines on how to prevent their clients from abusing the service provider’s resources. Each individual provider makes an assessment on a case-by-case basis as to whether the contract with his client or the provisions of the Electronic Communications Act provide him with an opportunity to shut down a service himself, or if he requires a legal decision in order to sanction his client.

Deleting the domain name linked to the content or service
If approaches to the holder and service provider are unsuccessful, for instance if the service is operated by an overseas provider, deletion of the domain name may represent a last resort. The deletion of a domain name will not remove the service, but it may reduce the harmful effects
it causes since the service will become less accessible.

In some instances it is not possible to contact either the holder or the service provider. In such cases, the registry for the top level domain in question can be contacted regarding deletion. The various top level domains operate with different requirements as to which criteria must be met in order to delete a domain name.

**What happens when a domain name is deleted?**

Deletion results in removal of the domain name from the domain name system. This means that you can no longer obtain the IP address for the service you have asked for when you look up the domain. Instead you receive an error notification telling you that the domain cannot be found. Deletion affects all services within the domain and all its sub-domains. However, this does not remove the content. The service is still available, but it will be considerably less accessible because the majority of Internet users are not aware of the IP address and will thus not be able to access the content.

Let us look at an example. A student has published illegal content on a web page belonging to the University of Oslo. Norid does not have access to delete either the web page, the student’s user space or an individual sub-domain. Our only option is to delete the domain name uio.no. The consequences of a deletion of this kind will be as follows:

- **All email addresses and web pages registered within the domain will cease to function**
  In the case of uio.no this will affect thousands of email addresses and a large number of webpages.

- **All name server computers within the domain will become inaccessible**
  This may affect other domains belonging to the University of Oslo. Furthermore, it may affect domains belonging to other organizations which use the university’s name servers for their own domains. For example, the Holocaust Centre’s domain, holocaust.no, relies on name servers within uio.no, and will thus cease to function.

- **All other services within the domain will become inaccessible**
  This may have negative spin-offs for services provided outside the domain. In our example, Feide (the Norwegian education sector’s personal identity administration system) will be affected, because this service utilizes student and employee databases at the various educational institutions in order to authenticate users. Those aspects of this service that require calls to databases at the University of Oslo will cease to function if uio.no is deleted.

- **All sub-domains will become inaccessible**
  The University of Oslo has several sub-domains, such as those linked to the various faculties, including jus.uio.no, matnat.uio.no and others, as well as those belonging to the university’s data security service UiO CERT (cert.uio.no). All these, together with their email addresses, websites and other services, will cease to function.

There are few domain names that have as many users and offer as many services as uio.no. The problem is that only the domain holder himself can know how many email addresses, web pages and other services are located within a domain. However, more detailed investigation of the holder’s activities might let an investigator estimate the likelihood of innocent third parties also gaining access to services linked to the domain.

Furthermore, there are several ways of reaching a service via the IP address. A simple approach is to set up a link directly to an IP address without going via the domain name system. Methods such as this are used by those who send junk mail (spam). It is also possible to set up several domain names pointing to the same service – for example within various top level domains. If one domain name is deleted, the others can be utilized for lookups the normal way. This means that even if uio.no is deleted, the illegal content may still be accessible via a .com domain, for example.
WHAT CAN BE DONE THROUGH NORID’S SYSTEMS?

Most of the aforementioned measures are taken outside the scope of Norid’s systems, whether in disputes over rights or disputes related to illegal services. Nevertheless, it is useful to have an overview of the steps that Norid can take using its own systems as regards a Norwegian domain name. The following operations can be carried out on a domain name using our systems:

- Update of contact information
- Modification of name servers
- Domain transfer to a new registrar
- Suspension of a domain
- Domain transfer to a new holder
- Deletion of a domain

Suspension:
The domain ceases to function, but remains registered by the holder.

Deletion:
The domain is removed from the database. Normally it will immediately become available to other applicants.

It is a precondition in the event of transfer that the new holder complies with the terms and conditions set out in the regulations.

VOLUNTARY MEASURES

A domain holder may request voluntarily that all of these operations be implemented on his domain name. This provides a rapid and effective means of conflict resolution in cases where the parties are in agreement.

MANDATORY MEASURES

Mandatory measures that can be imposed on a holder may be either temporary or permanent. In the case of a temporary measure, the subscription will not be terminated, but the holder’s user privileges to the domain will be strictly limited. The result of a permanent measure is that the holder loses his domain.

We require that the court or prosecuting authority provide us with a written decision that enables us to implement mandatory measures on a holder. It is important to note that Norid do not have to be involved as a party to the conflict in such cases. If the written decision is addressed to the holder, we can implement the operation pursuant to the agreement between ourselves and the holder. This presupposes that we have been informed of the decision, and that the wording makes it possible to implement the operation through our systems.

Temporary measures:
- Suspend the domain until the conflict is resolved.
- Impose limits on the holder’s rights to use the domain, for example by prohibiting deletion, transfer or other modifications before the conflict is resolved.
- Direct the subscriber to carry out operations on the domain, such as redirecting it to new name servers over which the opponent has control. Such actions may be relevant in criminal cases when the police may wish to assume charge of the technical function of the domain in order to conduct further investigations.

Note that an attempt to prohibit changing the registrar or name server will be more problematic. Both the registrar and the provider of the name service may be third parties, not involved in the conflict, with legitimate reasons to terminate the holder’s client accounts.

Suspension:
The domain ceases to function, but remains registered by the holder.

Deletion:
The domain is removed from the database. Normally it will immediately become available to other applicants.
To hold a domain name is regarded as a subscription, and an annual renewal fee is charged. The majority of registries, including Norid, will automatically delete domain names if the renewal fee is not paid. When a domain is suspended or if deletion is prohibited, it must at the same time be decided whether the holder or the opponent will be required to pay the renewal fee if payment is due during the conflict resolution process.

**Permanent measures:**
- Domain transfer to a new holder
- Deletion of a domain

It is important to note that the deletion of a domain does not prevent the holder from re-registering the same name. Norid’s automatic systems do not enable us to bar individual applicants from registering specific domain names. A new deletion requires a new legal decision unless the first decision expressly deprives the holder of all rights to utilize the domain in the future. In such cases, the opponent may contact us and request a new deletion by making reference to the original decision.

**Mandatory measures in civil cases**
The court can process domain-related conflicts in the same way as other conflicts even if the case in question has previously been brought before the Alternative Dispute Resolution Committee. Temporary measures will typically be in the form of temporary injunctions, while permanent measures will be handed down as part of a legal judgement. In cases where a legally binding decision has been made, the domain name policy provides the authority we need to either transfer or delete a domain name, or to carry out other operations without the holder’s consent. On the web page www.norid.no/domenekonflikt/rettssaker/ we have set out suggestions for claims worded in such a way that they can be implemented without coming into conflict either with the contract between Norid and the holder or any other form of regulation. (For legal reasons this document is available in Norwegian only).

**Mandatory measures in criminal cases**
Pursuant to Section 203 of the Norwegian Criminal Procedure Act, items regarded as having significance as evidence can be confiscated until such time when a legally binding decision has been reached. The same applies to items that are assumed liable to seizure from or mandatory surrender on the part of the aggrieved party. In a decision handed down by the Norwegian Supreme Court on 26 August 2009, a domain name was deemed to constitute an item in this context, and thus subject to confiscation. The prosecuting authority is in possession of the principal expertise enabling it to order such confiscation pursuant to Section 205 of the Norwegian Criminal Procedure Act in cases where “the holder refuses to surrender the item voluntarily”. However, any party affected by the confiscation can demand that a decision to carry out a confiscation be brought before the court, cf. Section 208 of the Norwegian Criminal Procedure Act.

In the case of a domain name, a confiscation will have the same effect as a suspension. In other words, the domain and the services within the domain will be rendered inaccessible, although the domain itself will still be registered by the holder in the database. For practical reasons, it is essential that we receive a written decision regarding confiscation from the prosecuting authority, and that we are informed if and when the confiscation order is rescinded.

A decision to confiscate is usually made for an indefinite period and will apply either until it is withdrawn or annulled by the court, or until a legally binding decision is made requiring the decision to be revoked. When the confiscation order expires, the holder regains his right to use the domain in the normal way.

During the period when the domain is under seizure, the prosecuting authority assumes responsibility for any expenses incurred.
In a criminal case, the confiscation of a domain may end with a legal decision involving permanent withdrawal as the final mandatory measure. Since the holder does not own the domain, but merely subscribes to it, withdrawal of a domain name will in practice function in a different way than if it had applied to his property. The domain has been employed as a "telephone number" to gain access to an illegal service, but is not in itself illegal. In the same way as for a telephone number it is thus the right to use the domain that is withdrawn, not the domain itself. The domain is deleted and remains part of the domain resource administered by Norid.

Since domain names are a limited resource, it is vital that as many as possible remain available to those who wish to acquire a domain name. At the same time there is a need to protect an unwitting third party from the burden of registering a domain name that has recently been involved in criminal proceedings. Our approach is thus to place the domain in quarantine for a certain period of time before making it available to new applicants.

Furthermore, as noted above, it may be appropriate for the prosecuting authority to argue in court that the holder be deprived of his user rights for a specified period so that the same judgement can be employed if the holder re-registers the domain.

On the website www.norid.no/domenekonflikter/beslag/ we provide information as to what Norid requires from the prosecuting authorities in the event of a confiscation order (in Norwegian only). Notification of a confiscation order or the rescinding of a confiscation order, as well as legally binding decisions regarding measures taken against a domain holder can be sent to us either via email or in the post.
UNINETT Norid AS
NO-7465 Trondheim

Office address:
Abels gt. 5, Teknobyen
Phone:  +47 07355
Fax:     +47 73 55 79 99
Email:   info@norid.no
www.norid.no/index.en.html

You will find this guide at
www.norid.no/publikasjoner/domenejus-en.pdf