NORID RUNS THE REGISTRY
FOR NORWEGIAN DOMAIN NAMES
norid.no

Domain conflicts
in the legal system

Norid AS
NO-7465 Trondheim

Location:
Abels gt. 5, Teknobyen
Phone: +47 73 55 73 55
E-mail: info@norid.no
www.norid.no

June 2019

NORID RUNS THE REGISTRY
FOR NORWEGIAN DOMAIN NAMES
norid.no

Domain conflicts
in the legal system

This guide is aimed at judges, prosecutors, police investigators, lawyers and others who may require specialized knowledge about the technical and practical aspects of conflict resolution and legal processes involving domain names.

This guide covers the following topics:

1. Organization of the internet address system
2. Who is responsible for what
3. When a conflict arises
4. Relevant measures in our systems

What is a domain name?

A domain name—or a domain—is an address on the internet. It is normally used for websites and e-mail. Registering a domain name gives the holder the right to use the name for as long as the subscription is active.

1. Organization of the address system

For internet users, it is the services operating on the technical infrastructure that have value. Among these services, the most well-known include websites and e-mail, but it is also possible to use the net to connect phone calls, download files, log on to various databases, etc.

So, how do we access these services? All devices connected to the internet have their own unique IP address, which consists of a long sequence of numbers. It is possible to use this address to connect directly to a device, but to save users from having to remember these number sequences, the Domain Name System (DNS) attaches a unique domain name to the IP address in question.

The domain name system is the "telephone book" of the internet.

You look up a name in the telephone book to find the corresponding telephone number. The same approach is used in the domain name system; domain names are used to look up IP addresses. The lookup process initiates a search for the IP address, which is used to connect your device to the service you want to access. We all know that a telephone call is not conducted through the telephone book. Similarly, internet traffic does not pass through the domain name system.

Norwegian domain names end in .no. The format is *mydomain.no*, where **mydomain** is whatever domain name you have chosen. If your domain name is used to provide services such as websites and e-mail, its address may be *www.mydomain.no,* and a typical e-mail address may use the format *firstname.lastname@mydomain.no* or *mail@mydomain.no*.

Please note that a domain name may be registered without having any services associated with it. It is a requirement that all Norwegian domains be in good working order, technically speaking, but the domains are not required to include any content in the form of websites or e-mail addresses.

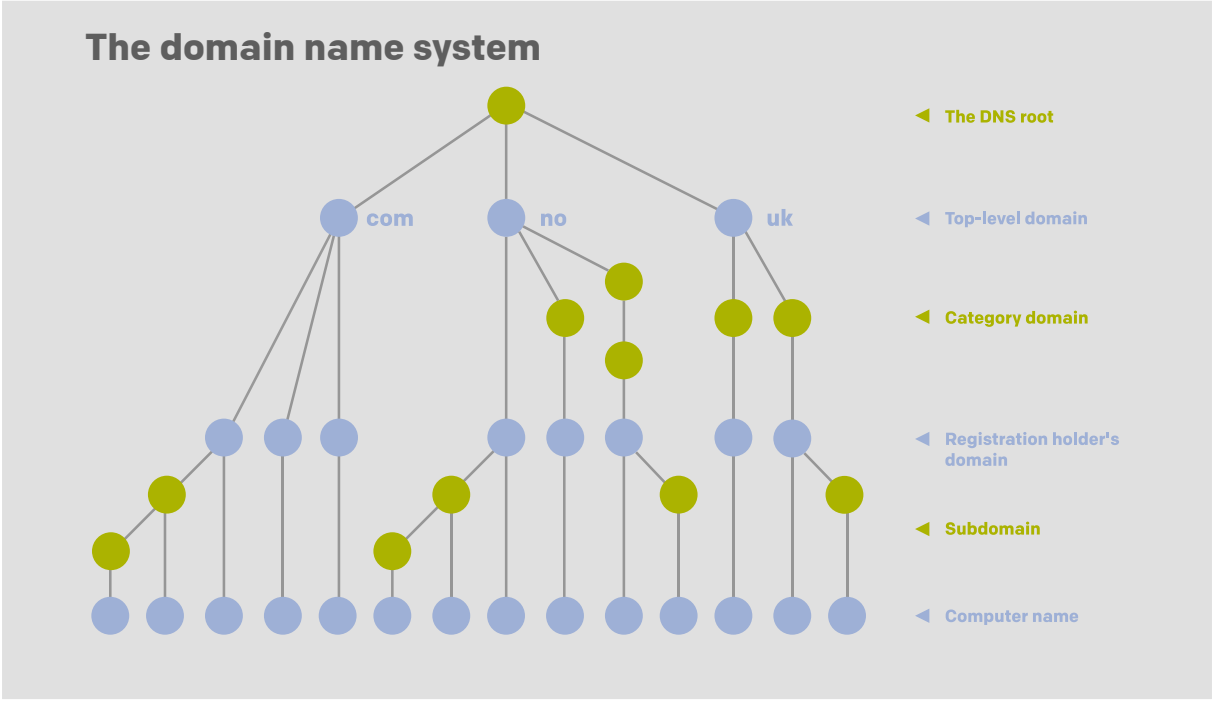
A domain name is always unique. *Regjeringen.no* and *regjeringa.no*, for example, are two different domain names, because their spelling is different. This applies even if the two names mean the same thing, have been registered by the same organization and point to the same IP address.

Organization of the domain name system

The domain name system is structured like a hierarchy and can be compared to the roots of a plant. At the very top is what is often called the DNS root zone, or just the "root".

The level just below the root is what is called the top-level domain. There are two different types of top-level domains. One is country codes, such as .no (Norway) and .se (Sweden). These are subject to regulations drawn up at national level. The other is generic top-level domains, including .com, .org and .net. These are subject to regulations established by international agreement.

Below the top-level domains is the level we normally think of when we hear the term domain name, such as *uio.no* for the University of Oslo. Some top-level domains also have so-called category domains at this level. Category domains are reserved for specific groups, such as *dep.no* in Norway, which is the category for Norway's government ministries, or *priv.no*, which is the category domain for private individuals. At the next level down are so-called sub-domains, such as *minestudier.uio.no* and names of computers, such as *stream-prod02.uio.no*.



The root structure also reflects levels of responsibility. Separate organizations are responsible for the various "rootlets" at each level. Different registries administer and operate the central database for each individual top-level domain. Norid AS, or Norid for short, is the administrator of the .no top-level domain.
The user who has registered a Norwegian domain name (the holder) is free to create sub-domains under this domain name.

Individual users can only influence rootlets immediately below their own level in the hierarchy. This means that Norid, for example, cannot influence the .com top-level domain or any domain name registered under this top-level domain.

Top-level domains worldwide

On our website we maintain a list of registries responsible for the other top-level domains around the world. Use this list if you need to contact someone about a domain outside .no.

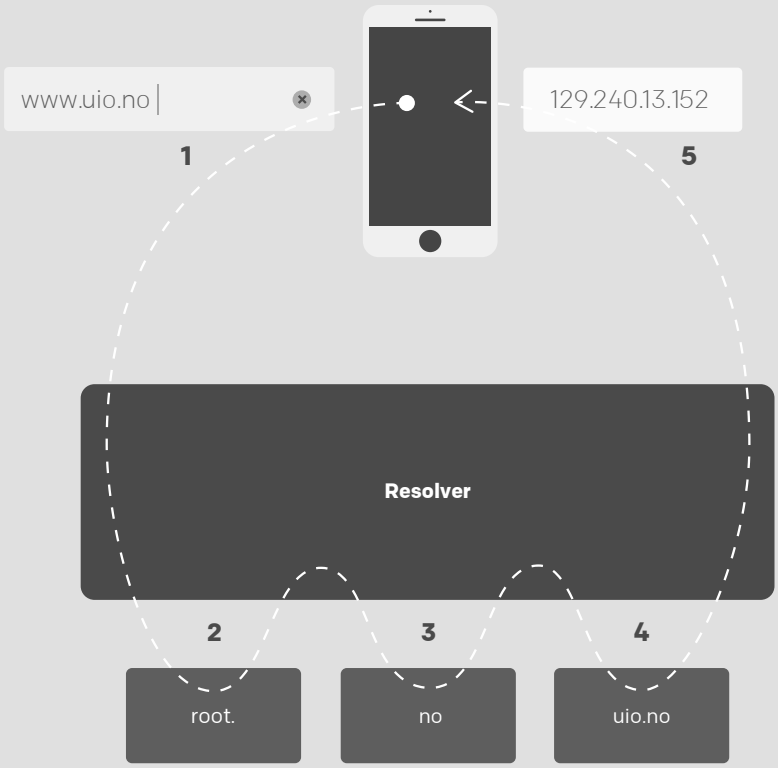
www.norid.no/en/om-domenenavn/domreg/

What happens when a domain name is looked up?

Each domain name has a set of servers handling queries about addresses under the name in question. These servers are called name servers.

For the most part, the user is unaware of the communication that goes on with these servers.

What happens behind the scenes when you look up a domain?



Say you want to look up information about a specific event on the University of Oslo's website. You know that the university's address is *www.uio.no*, so you enter this address into your browser.

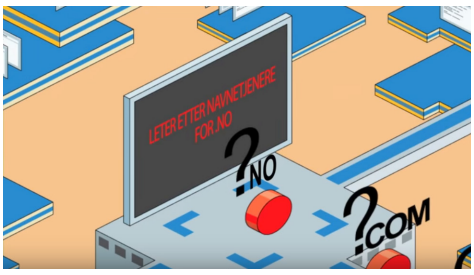
1. A small application in your device contacts a dedicated server set up to handle queries in the domain name system, a so-called recursive resolver. This server is often operated by your internet service provider.

2. The recursive resolver is tasked with finding the IP address of *www.uio.no*. It forwards the query to one of the name servers for the root of the domain name system. Root name servers only know the level below them in the hierarchy, and therefore returns a list of name servers for the top-level domain .no.

3. The resolver then forwards the query to one of the name servers for .no. These servers also only know the level below them, and therefore return a list of name servers for *uio.no*.

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

5. The resolver then forwards the IP address to your device. Once your browser is provided with the IP address, it contacts the university's web server and downloads the website you requested.



This video demonstrates how the domain name system works:
https://www.norid.no/en/video/slik-virker-domenenavnsystemet/

2. Who is responsible for what?

Our focus here is Norwegian domain names, which are domain names ending in .no. All domain names immediately below the top-level domain have been registered in Norid's database. As at September 2017, this number is approx. 740,000. Every month, we process approx. 10,000–12,000 applications for new domain names.

Framework

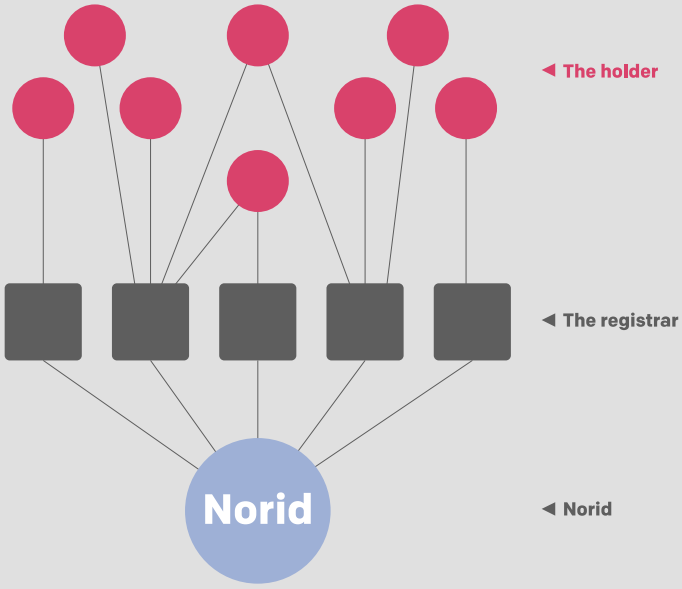
Norway's top-level domain is administered in accordance with national regulations, cf. Section 7-1 of the Electronic Communications Act[1], and the Norwegian Domain Regulations[2]. These regulations set the boundaries[3] for Norid's work on developing and amending[4] [5] the domain name policy for .no.

The Norwegian registration service has been fully automated for many years, in order to streamline the process and meet user needs for swift processing of applications. Before registering, the applicant submits a personal declaration,[6] where he confirms that he is not infringing on the rights of any third party, and that he assumes full responsibility for the consequences of his registration and use of the domain name in question. There is no pre-screening in this process. Any claims of infringement or other disputes are handled after the fact, either by the Alternative Dispute Resolution Committee or by the courts.

Parties, roles and responsibilities

A domain is created as soon as Norid registers the domain to an organization or an individual. The holder is granted the right to use the domain name for as long as the registration is valid, normally until the organization or individuals terminates it.

Who is involved?

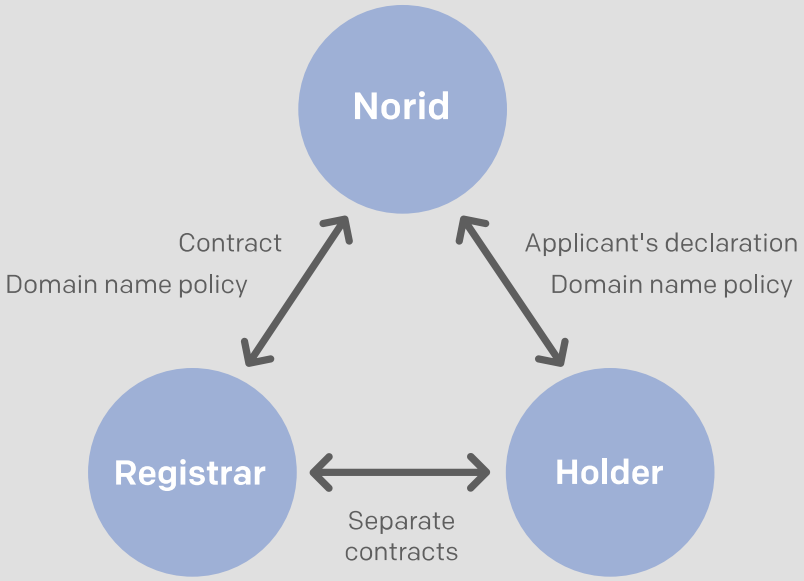


Three parties are involved in the registration of domain names:

1. **The holder,** who is the individual or organization seeking to register the domain name.
2. **The registrar,** who submits applications on behalf of the holder, acting as the intermediary between the holder and Norid.
3. **Norid,** who processes the application in accordance with relevant regulations, enters the domain in the central register and operates the name server for .no.

The relationships between the holder, registrar and Norid is regulated by private-law agreements. The domain name policy for .no acts as both a contract between Norid and the holder, and between Norid and the registrar. In addition, Norid has a separate contract[7] with registrars. The rights and duties under the domain name policy for .no are always vested in the holder. This applies even in cases where the holder has allowed a third party to use his domain or create subdomains.

Contractual relationship between the parties



The holder is responsible for everything his registration is used for. Norid does not monitor website content, nor does it have any authority to impose sanctions on websites that appear to break the law; this authority lies with the police and the legal system[8].

How to find the holder of a specific domain

Norid runs a lookup service for Norwegian domains: *www.norid.no/en/domeneoppslag/hvem-har-domenenavnet/.* Here, you can find out who the holder is and see which, if any, other domains the holder has. The lookup service also provides information about the name servers hosting the domain, the name of the person to contact about technical matters, and the name of the registrar. Some of this information may point to the the identity of the technical provider of services under the domain.

3. When a conflict arises

Services offered by domain names and website content are subject to Norwegian law. The domain name holder bears full legal responsibility for how the domain is used. The holder is free to decide whether the domain will be offering services, and, if so, which services the domain will offer. These may be services set up by the holder himself within his own organization, using his own computers, or he may choose to purchase products from an internet service provider or other service providers. Services may vary in terms of content—from static websites to websites offering content for download, online games, blogs, portals (such as *altinn.no*) and a wide range of other services.

Domain names typically become involved in two types of conflicts: The first are conflicts where the domain name itself is at the crux of the dispute, and the second are conflicts where the domain name is involved because it leads to disputed content. Norid is normally not a party to these conflicts, nor does it have to be in order to implement necessary measures.

Domain name disputes

For the most part, these are civil suits where the dispute centres on which party has the right to use the domain. In principle, this type of dispute would also extend to cases where a party claims a domain name in itself is slanderous or unlawful.

Content- and service-based disputes

In crimes and other unwanted activity on the internet, more often than not the services are the problem, not the domain name itself. Both websites and e-mails may include unlawful content or be used for unlawful activities, such as attempted fraud. These types of conflicts tend to end up as criminal cases, where the prosecuting authority is looking to shut down to a certain type of content or service. Sometimes other parties—public or private—want to shut down the content of a website.

Relevant measures in domain name disputes

Disputes concerning rights to a domain name may be brought before a court of law. For Norwegian domain names, the Alternative Dispute Resolution Committee is a fast, cost-effective and simple alternative in straightforward disputes.

The ADR Committee may decide that a domain name is to be transferred to a new holder or deleted. In their contract with Norid, domain name holders have committed to taking part in the complaints process and to being bound by the Committee's decision. If either party is unhappy with the decision, the dispute may be brought before a court of law. A decision handed down by the ADR Committee is not binding for the court going forward.

Alternative Dispute Resolution Committee

The ADR Committee is an independent body, hearing disputes concerning rights to Norwegian domain names and complaints concerning decisions made by Norid. In its role as secretariat for the Committee, Norid is responsible for preparing case documents, but makes no submissions about the cases themselves. All Committee decisions are posted on both Norid's website and Lovdata.

Alternative Dispute Resolution Committee: *www.norid.no/en/om-domenenavn/spesialiststoff/domeneklagenemnda/*
Complaints archive: *www.norid.no/no/om-domenenavn/spesialiststoff/domeneklagenemnda/klagearkiv/ (Norwegian only)*
Court decisions archive: *www.norid.no/no/om-domenenavn/spesialiststoff/rettslig-behandling/rettssaker/ (Norwegian only)*

Relevant measures in content- and service-based disputes

The only effective means of making an unlawful service entirely inaccessible without negatively affecting third parties, is to remove the content or shut down the service. This can only be done locally, on the computers where the service is provided. Consequently, the most effective approach is always to take steps aimed directly at the domain name holder or to contact the service provider.

1. Contact the domain name holder
The natural starting point in a dispute involving content or services on the internet is the domain name holder. Some disputes are resolved by the holder voluntarily removing the content or shutting down the disputed service.

If this approach is not successful, legal action is an alternative recourse in forcing the holder to shut down the service in question.

Slettmeg.no: Guidance service of Norwegian Center for Information Security

The Norwegian Center for Information Security (NorSIS) offers a guidance service, *slettmeg.no*, about how to proceed if you have encountered offensive or abusive content online.They are quite knowledgeable about what it is possible to remove and how to proceed in order to succeed.

Guidance service offered by the Norwegian Center for Information Security: *www.slettmeg.no*

E-mail: hjelp@slettmeg.no

Telephone: 08247

2. Contact the service provider
If it is not possible to contact the domain holder, the next step is to contact the service provider. In many cases, this will be the internet service provider.

Most Norwegian ISPs have guidelines in place to prevent their customers from abusing their resources. The individual service provider will consider, on a case-by-case basis, whether the service can be shut down based on provisions in the contract with the customer or the Electronic Communications Act, or whether a court order is required for them to act.

3. Delete the domain name linked to the content or service
If approaching the domain name holder or service provider is not successful, perhaps because the service is provided by a provider in another country, deleting the domain name may be your only recourse. Deleting the domain name will not remove the unlawful service, but it may help control the damage by making it less accessible.

Sometimes it is not possible to contact either the domain name holder or the service provider. In these cases, you may submit an application to the registry for the top-level domain to have the domain deleted. The various top-level domains operate with different criteria that have to be met in order for a domain name to be deleted.

Deleting a domain name means having it removed from the domain name system. This means that you will no longer get an IP address for the service when you look up the domain; instead you get an error message informing you that the domain no longer exists. Deleting a domain affects all services within the domain and any subdomains linked to it. However, this does not mean that the content is gone. The service still exists, but it will be less accessible, as most internet users are not aware of the IP address and will therefore not be able to access the content.

What happens when a domain name is deleted?

Let's say, for example, that a student has posted illegal content on a web page on the University of Oslo's domain. Norid does not have the authority to delete the web page itself, the student's user pages or a single subdomain. All we can do is delete the domain name *uio.no*. This will have far-reaching consequences:

- **All e-mail addresses and web pages linked to the domain will stop working**
  For *uio.no*, this would affect thousands of e-mail addresses and a considerable number of web pages.
- **All name server computers within the domain will become unavailable**
  This may affect other domains belonging to the University of Oslo. Furthermore, it may also affect domains belonging to other organizations, which use the university's name servers for their domains. This includes, for example, the domain of the Center for Studies of Holocaust and Religious Minorities, holocaust.no, which will stop working.
- **All other services within the domain will become inaccessible**
  This may cause a ripple effect and affect services provided outside of the domain. In our example, Feide, which is the joint identity management system for the Norwegian education sector, would be affected, because this service relies on student and employee databases at educational institutions to authenticate users. The parts of the service requiring access to databases at the University of Oslo will cease to function if *uio.no* is deleted.
- **All subdomains become inaccessible**
  The University of Oslo has a number of subdomains, including faculty subdomains (*jus.uio.no*, *matnat.uio.no*, etc.) and the university's Computer Security Incident Response Team (cert.uio.no). All of these subdomains, including e-mail addresses, web pages and other services, will cease to function.

Few domain names have as many users and services as our example above. The problem is that only the domain name holder will know how many e-mail addresses, web pages and other services are located within a domain. A more detailed investigation into the domain name holder's activities would reveal, however, how likely it is that innocent third parties use services linked to the domain.

Furthermore, there are several ways of reaching a service through the IP address alone. The simplest way is to link directly to an IP address without going through the domain name system. This strategy is used by those who send junk e-mail (spam). It is also possible to set up several domain names so that they point to the same service, such as through several top-level domains. If one domain name is deleted, the others can still be used for lookups. This means that the unlawful content may still be accessible, for example through a .com domain, even after the .no domain has been deleted.

Learn more about content and domain name conflicts on the Internet:
www.norid.no/en/video/ulovlig-innhold-pa-nettet/

4. Relevant measures in our systems

Most of the steps that should be taken, whether in disputes over rights or disputes involving unlawful services, take place outside of Norid's systems.

Nevertheless, it is useful to have some idea of the steps Norid can take against a domain name within its own systems.

Voluntary measures

There are a number of things a domain name holder can request Norid to implement for his domain. If the parties can reach an agreement, this is a quick and cost-effective way to resolve a conflict.

What can be done about a domain?

- Update contact information
- Modification of name servers
- Transfer the domain to a new registrar
- Suspend the domain
- Transfer the domain to a new domain name holder
- Delete the domain

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

Transfer: The new domain name holder must meet criteria established by the domain name policy.

Deletion: The registration is deleted, and the domain is removed from the database. Normally, this means that the domain becomes available to other applicants immediately.

Injunctions against the domain name holder

Everything a domain name holder can voluntarily request to have done about his domain, can also be ordered or prohibited as part of an injunction against the domain name holder.

Norid requires a written order from the court or prosecuting authority to implement injunctions against the domain name holder. Please note that it is not necessary to make Norid a party to the dispute in these cases. The written order should be addressed to the domain name holder, and in accordance with the contract between us and the domain name holder, we implement the measures. This requires that we have been notified of the order, and the wording of the order must make it possible for us to implement the measures in our systems.

Injunctions include both measures that are implemented during a dispute, and measures that are implemented upon settlement of the dispute.

While the dispute is ongoing, we can

- suspend the domain until the dispute is settled
- limit the domain name holder's control of the domain, e.g. by preventing the holder from deleting, transferring or changing the domain before the dispute is settled
- transfer control of the domain to another party until the dispute is settled. This may be relevant in criminal cases.

Please note that imposing restrictions on switching registrars or name servers could be problematic. Both registrars and name server providers may be third parties that are not part of the dispute, and these parties may have a legitimate reason to terminate their customer relationship with the domain name holder.

Domain name registrations are subject to an annual renewal fee. Most registries, including Norid, will automatically delete domain names if the renewal fee is not paid. If a domain is suspended or if deletion is prohibited, a decision must be made whether the domain name holder or the opposing party will be liable to pay the renewal fee if this falls due before the dispute is settled.

After the dispute has been settled, we can

- transfer the domain to a new domain name holder
- delete the domain

Please note that deleting a domain does not prevent the domain name holder from registering the domain again. Our automated systems does not allow us to bar individual applicants form registering specific domain names.

Civil cases
The courts hear all domain-related disputes in the same way as other disputes, even if the case has previously been heard by the ADR Committee. In order to provide quick and cost-effective dispute resolution while ensuring due process, the Committee only hears disputes within a clearly-defined, limited framework. When a dispute is brought before a court of law, however, the Committee's decision is set aside for a full hearing of the dispute. Arguments and evidence not presented before the Committee may be submitted in court. The Committee's decision may serve as a kind of expert witness report, but it does not in any way limit the court in its assessment of the various aspects of the case.

In civil suits, measures implemented before the dispute is settled normally take the form of an interim court order, whereas measures implemented upon settlement of the dispute take the form of a judgment or final ruling.

When a final and enforceable decision has been handed down, Norid has the authority to transfer or delete a domain or implement other measures without the domain name holder's consent. It is a condition, however, that the wording of the decision must enable Norid to implement the measures without violating the provisions of the contract between us and the domain name holder in other respects, or the provisions of the domain name policy in general.

Recommended phrases in civil cases:

www.norid.no /no/om-domenenavn/spesialiststoff/rettslig-behandling/pastand-sivilsaker/
(Norwegian only)

Criminal cases
Pursuant to Section 203 of the Criminal Procedure Act, objects deemed to be significant as evidence may be seized until a legally enforceable judgment is passed. The same applies to objects that are deemed to be liable to confiscation or to a claim of surrender by an aggrieved person. The Supreme Court has ruled that domain names are considered objects in this context, and therefore subject to seizure9. Under Section 205, the prosecuting authority may order seizure of any objects "the possessor will not surrender voluntarily". Anyone affected by a seizure, however, may demand, pursuant to Section 208, that the seizure order be reviewed by a court of law.

For domain names, the registration is what is seized, by the police taking control of the it until the case is final. Norid is not a party to these cases, but because we operate the register of Norwegian domain names, we must register that control of the registration has been transferred. The seizure is addressed to the domain name holder, and the prosecuting authority's decision is forwarded to us in writing. The registration is then transferred, and the police is registered as the domain name holder, with the rights and duties this entails.

While the domain is under seizure, the police are responsible for keeping the registration active so that it can be returned later on, and the police is liable for transfer fees and any other costs that may accrue.

Seizures remain in effect until they are lifted or otherwise reversed. Once the seizure is lifted, the police must transfer the registration to the original domain name holder, or any other party identified by him. Registration is transferred in accordance with standard procedures for the transfer of domains.

In a criminal case involving seizure of a domain name, the court may order forfeiture as a final measure. In that the domain name holder does not own the domain, but simply subscribes to it, forfeiture of the domain name will, in practice, differ from other forfeitures. The registration has been used to offer an address for an unlawful service, but the domain itself is not unlawful. Similar to how it would work for telephone numbers, the domain name holder forfeits control of the domain, not the domain itself. Once the registration is deleted, the domain becomes part of the domain resource managed by Norid.

Domain names are a limited resource, and it is important that as much of this resource as possible remains available to those who wish to acquire a domain. At the same time, however, it is important to protect third parties from the stigma of unknowingly registering a domain name that recently has been associated with a criminal case. Our policy is therefore to quarantine the domain for some time before making it available to other applicants.

Guidelines for the police and prosecuting authority in connection with seizures of Norwegian domains:

Seizure: *www.norid.no/en/konflikt-om-domene/veiledning-til-myndigheter/beslag/*

Forfeiture: *www.norid.no/en/konflikt-om-domene/veiledning-til-myndigheter/inndragning/*

Source:

1 Electronic communications act § 7-1
https://lovdata.no/dokument/NL/lov/2003-07-04-83/KAPITTEL_7#§7-1 (Norwegian only)

2 The domain regulation
https://lovdata.no/dokument/SF/forskrift/2003-08-01-990 (Norwegian only)

3 The administrative model for .no
https://www.norid.no/en/om-domenenavn/spesialiststoff/rammeverk/forvaltningsmodell/

4 The policy development process for .no
https://www.norid.no/en/om-domenenavn/spesialiststoff/rammeverk/regelverksprosess/

5 The domain name policy for .no
https://www.norid.no/en/om-domenenavn/regelverk-for-no/

6 Applicant's declaration
https://www.norid.no/en/om-domenenavn/regelverk-for-no/vedlegg-g/

7 The registrar agreement
https://teknisk.norid.no/no/registrar/ordning/avtale/

8 HR-2009-01692-U
https://www.norid.no/uploads/2019/06/hr-2009-01692-beslag-en.pdf

9 HR-2009-01692-U
https://www.norid.no/uploads/2019/06/hr-2009-01692-beslag-en.pdf