Implementation of NIS2, Article 28 .dk domain names

Model for Collection, Verification and Publication
of
Domain Name Registration Data

Introduction

The European NIS2 Directive, Article 28, introduces a new obligation to collect and maintain correct and complete registration data (WHOIS obligation). A working group has been established between registrars and Punktum.dk to find a common model for complying with the new WHOIS obligation to avoid duplication of work for the benefit of registrants, registrars and registry.

The working groups solutions is presented in this consultation material. The material consist of:

- Model for implementation of NIS2, Article 28, in relation to .dk domain names (Current presentation)
- Approved verification methods (Appendix 1)
- Technical solutions (Appendix 2)

Current presentation introduces the new WHOIS obligation in NIS2, Article 28, and the relationship between Article 28 and the Danish Domain Act. The two legislations forms the basis for the collaboration between registrars and Punktum dk.

Hereafter the working group and its terms of reference, which have framed the work, is introduced. Used terminologies will be explained and the different solutions will hereafter be presented using simple and detailed flowcharts.

Summary of proposed solutions

Below is an overview of the working group's solutions on how to collect and maintain correct and complete data of a registrant. Punktum dk will publish the registrant's data in the public WHOIS on Punktum dk's website. Publication of .dk domain name data will as something new include email, if the registrant is a company. The current registrar agreement will be updated to make verification of data by registrars possible. This will be new. Punktum dk will be able to audit verifications done by registrars.

Data	Activity	When	Who	How
Name Address Phone number E-mail	Collecting data	A new user is created	Registrar collects data upon creation of a user	Registrar sends collected data to registry >> registry creates user and notify registrar (same as today)
	Maintaining data (update of data)	User wants to update data	If the registrant is managed by the registrar, the registrar updates data (registrar management)	Updated data is sent from registrar to registry (same as today)*
			If the registrant is managed through Punktum dk, Punktum updates the data (registrant management)	No information is sent to registrar (same as today)
	Verification of user data	Before creation of a user	Registrar can always verify user data before creation of a user	Together with new user data, registrar sends verification status to registry (this is new)
		After creation of a user	If the user is managed by the registrar >> registrar can choose to verify data >> if so, registrar verifies data	The option is set in the registrar's profile in EPP >> registry notify registrar, if verification is necessary (this is new)
			If the user is managed by the registrar >> registrar can choose that the registry do the verification >> if so, registry verifies data	The option is set in the registrar's profile in EPP >> registry notifies registrar about status and result of verification (this is new)
			If the user is managed through the registry >> verification is always done by the registry	No notification to registrar (same as today)

* If the registrant resides in DK, data will as a main rule be locked to CPR/CVR. If registry receives updated data from CPR/CVR updated data will be sent to registrar. No additional verification is necessary.

NIS2 Article 28's new WHOIS obligation

For the purpose of contributing to the security, stability and resilience of networks and information systems the NIS2 Directive, Article 28, imposes a new WHOIS-obligation on registrars and registries. NIS2 is expected to be implemented into Danish Law at the end of 2024. Below is text extract from the provision:

- **Article 28 (1)** requires "*… TLD name registries and entities providing domain name registration services to **collect and maintain accurate and complete domain name registration data**…*"
- **Article 28 (3***) requires "..the TLD name registries and the entities providing domain name registration services to **have policies and procedures**, including **verification procedures**, in place…*"
- ***Article 28 (4)** requires "…the TLD name registries and the entities providing domain name registration services to make **publicly available**, without undue delay after the registration of a domain name, the domain name registration data which are not personal data."*
- ***Article 28 (5)** requires "… TLD name registries and the entities providing domain name registration services to **provide access to specific domain name registration data** upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection law."*
- **Article 28 (6)** states that "*Compliance with the obligations laid down in paragraphs 1 to 5 shall not result in a duplication of collecting domain name registration data. To that end, Member States shall require TLD name registries and entities providing domain name registration services to **cooperate with each other.**"*

WHOIS obligation in NIS2 and Danish Domain Act

While NIS2, Article 28, introduces a new obligation to ensure accurate and complete data on the registrant and the point of contact administrering the domain name (proxy), if not the registrant, the Domain Act already obliges Punktum dk to ensure accurate and up-to-date data on a registrant. Below is shown which data must be verified according to the two legislations:

Data	Registrant	Point of contact (proxy)
Name	NIS2 + Domain Act	--- No obligation –
Phone number	NIS2 + Domain Act	NIS2
Email	NIS2 + Domain Act	NIS2
Address	Domain Act	--- No obligation –

As both NIS2, Article 28, and the Domain Act contain an obligation to ensure accurate data, the solutions of the working group includes all data mentioned in Article 28 and the Domain Act in order to cooperate.

NIS2 working group between registrars and registry

Article 28 in the NIS2 Directive states that registries and registrars must cooperate with each other to avoid duplication of work.

A working group with registrars was established in the spring of 2023. The group has been open for all registrars. Below is a list of registrars, who have participated in the working group:

- CSC
- Gandi
- INWX
- Mark Monitor
- One.com/Group One
- Simply
- Team.blue
- Tucows
- Openprovider
- Central Nic
- OVH Cloud
- Ascio

There have been 2 working groups. One has focused on finding common solutions regarding Article 28 and the second on the technical implementation.

Terms of reference for the working group

The purpose of the working group has more concrete been to find a model for how registrars and Punktum dk can cooperate in regard to :

1. Collecting and maintaining Domain Name Registration Data
2. Ensuring correct and complete Domain Name Registration Data
3. Publication of Domain Name Registration Data
4. A technical solution on how to share necessary data
5. Compliance and audit

Registrars and the registry are not cooperating regarding the requirements to have policies and procedures in place (art. 28 (3)) and, to give access to legitime access seekers (art. 28 (5)). Registrars and the registry must each find solutions to these obligations.

Terminology (1)

Point of contact
Is a natural or legal person administering the domain name on behalf of the Registrant, e.g. an appointed proxy

User is created
User data is sent and registered at registry

Domain name is created
Domain name is registered at registry after accept of Punktum dk's terms and conditions

Domain name is activated
Domain name is activated in the .dk-zone after completed data and ID-control, if required

Validation
Data validation ensures that data complies with the expected format. It typically comprises syntax checks (i.e. postal code) or the formatting of email addresses

Verification
Data verification evaluates whether data correctly reflects the attributes of the registrant (such as their identity or postal address). It aims to establish the accuracy of the claimed identity and data of the registrant.

Terminology (2)

Registrar transfer
When a domain name transfers from one registrar to another registrar

Registrant transfer
When a domain name transfers from one registrant to another registrant

Registrar management
When a registrant has authorized the registrar to take certain actions on behalf of the registrant, e.g. make payment to Punktum dk in connection with a conclusion of agreement and renewal and extension thereof

Registrant management
When a registrant may take certain actions himself to manage the right of use to a domain name directly through Punktum dk. In this case the costumer is "owned" by the registry.

Domain name registration data
Domain name registration data includes, according to NIS2, Article 28: Domain name, date of registration, registrant's name, contact email address and telephone number and contact email address and telephone number of the point of contact administering the domain name, in the event that they are different from those of the registrant. In this context domain name registration data also includes address of a registrant.

Terminology (3)

DK resident

A natural or legal person with residence in Denmark. Will as main rule be locked to CPR (Central Personal Register) or CVR (Central Business Register)

Non-DK resident

A natural or legal person with residence outside Denmark. Will not be locked to CPR or CVR

Risk assessment

Punktum dk will assess the risk that a Non-DK resident has provided data that is not correct. The assessment is based on several different parameters. If the risk score is below a given threshold, verification will not be required. If the risk score is above the threshold, verification will be required.

Solutions on collecting and Maintaining Domain Name Registration Data (1)

Main principles

- Known models should, as far as possible, be used to make it easy for registrants, registrars and registry to comply with the requirement to collect and maintain accurate domain name registration data.

- Registrar collects registrant data and maintains data if the registrant is managed by the registrar as today.

What data is collected

Registrant

- Name
- Address
- Phone number
- Email

Point of Contact (proxy)

- Name
- Address
- Phone number
- Email

What data is maintained

Registrant

- Name
- Address
- Phone number
- Email

Point of Contact (proxy)

A domain name can only be managed by a proxy, if the domain name is registrant managed. Therefore, only registry will maintain data of a proxy

Who collects and maintain data

Collecting data:

- Registrar collects data upon registration of a user

Maintaining data:

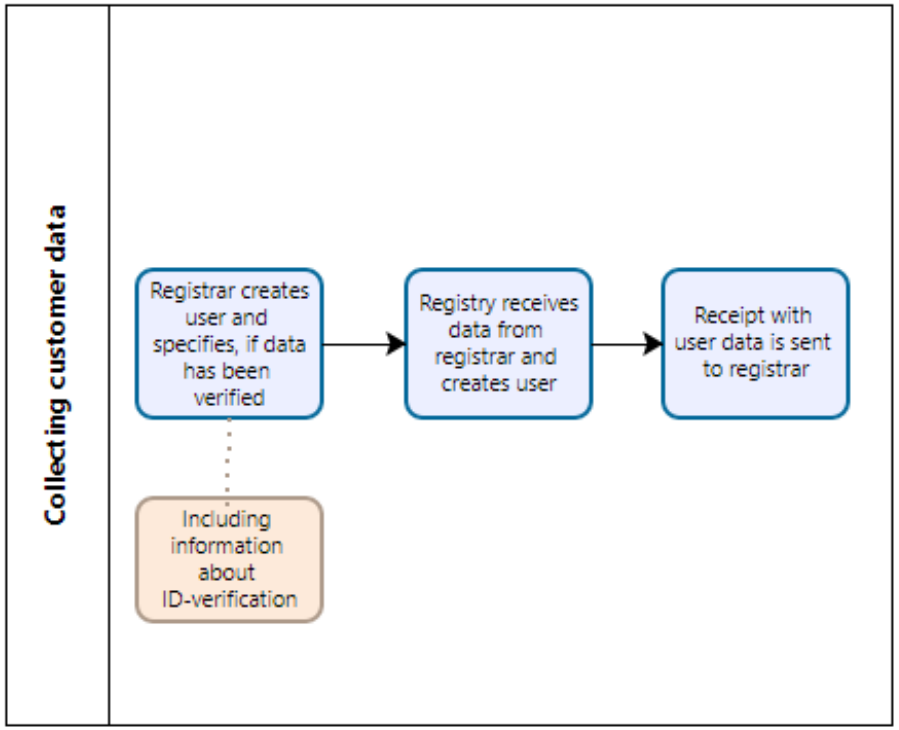
- If the domain name is managed by the registrar, the registrar maintains updated data
  - Exemption 1: Update of name, e.g. if change of last name, is done by registry. Registry sends updated name to registrar. (If registrar want to change name/identity, it must be done by transferring the domain name.)
  - Exemption 2: Registrant resident in DK where name and address is locked to Central Personal Register (CPR) or, Central Business Register (CVR), registry sends updated name and address to registrar
- If the domain name is in "registrant management", Punktum dk maintains updated data

Creation of a new user (simple flow chart)

Distinction between creation of a user and registration of a domain name is made, due to the fact that the user is not always a registrant, where verification is necessary. When a new user is created, it is done before the domain name is registered.

Process:

- Registrar creates user and specifies, if data has been verified
- Registry receives data from registrar and creates user
- Receipt with user data is sent to registrar



Update of user information (simple flow chart)

It is only relevant to share updated data on the user, if the user is managed by the registrar ("registrar management"). If a registrant has chosen to manage the domain name ("registrant management"), Punktum dk will update the user's data.

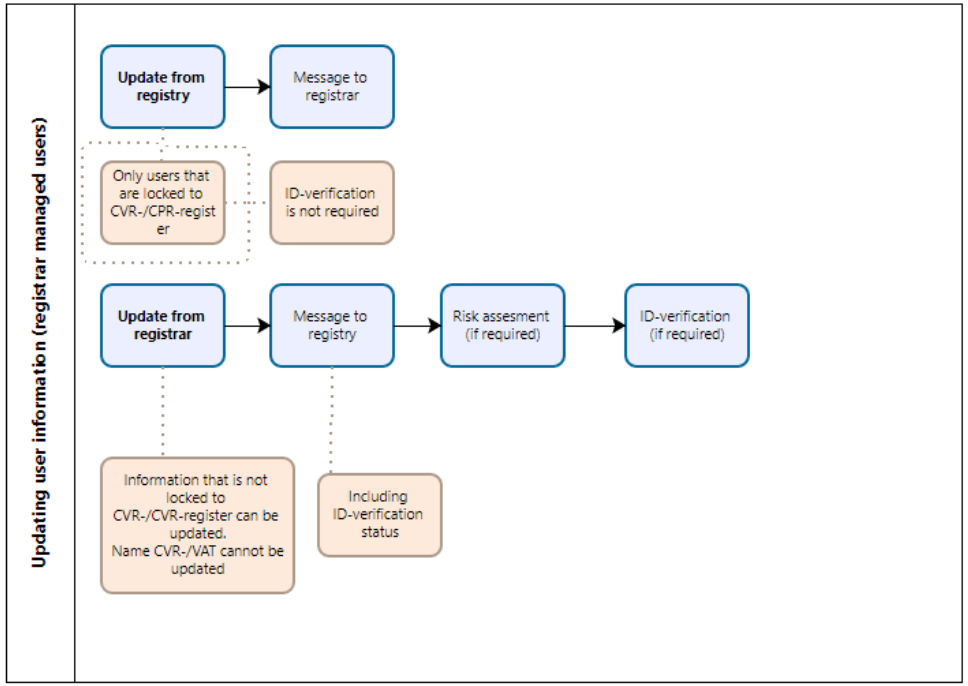
Process registrar managed user

<u>If data is locked to CVR/CPR (DK resident)</u>

- Registry receives updated data from CVR/CPR and sends data to registrar, > verification is not required

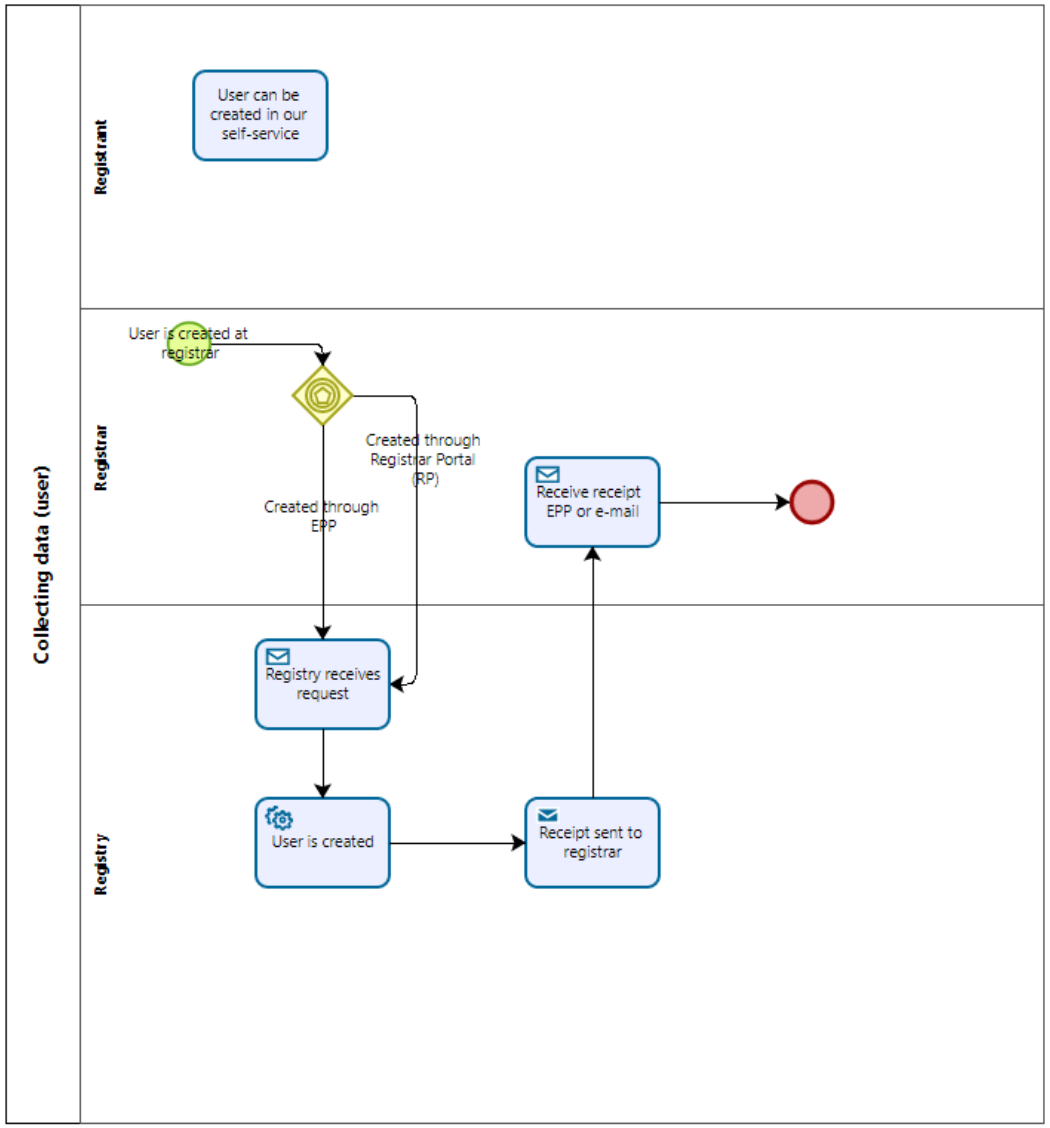
<u>If data is not locked to CVR/CPR</u>

- Registrar sends updated data to registry, including verification status. If user is:
- <u>Non-DK resident</u>
  Registry makes a risk assessment of the data, unless the registrar has already verified data.
  Risk assessment can require a verification of the registrant.
- <u>DK resident with protected name and address or registrant moving to Denmark.</u>
  The registrant must complete a new MitID-control, if update concerns address.



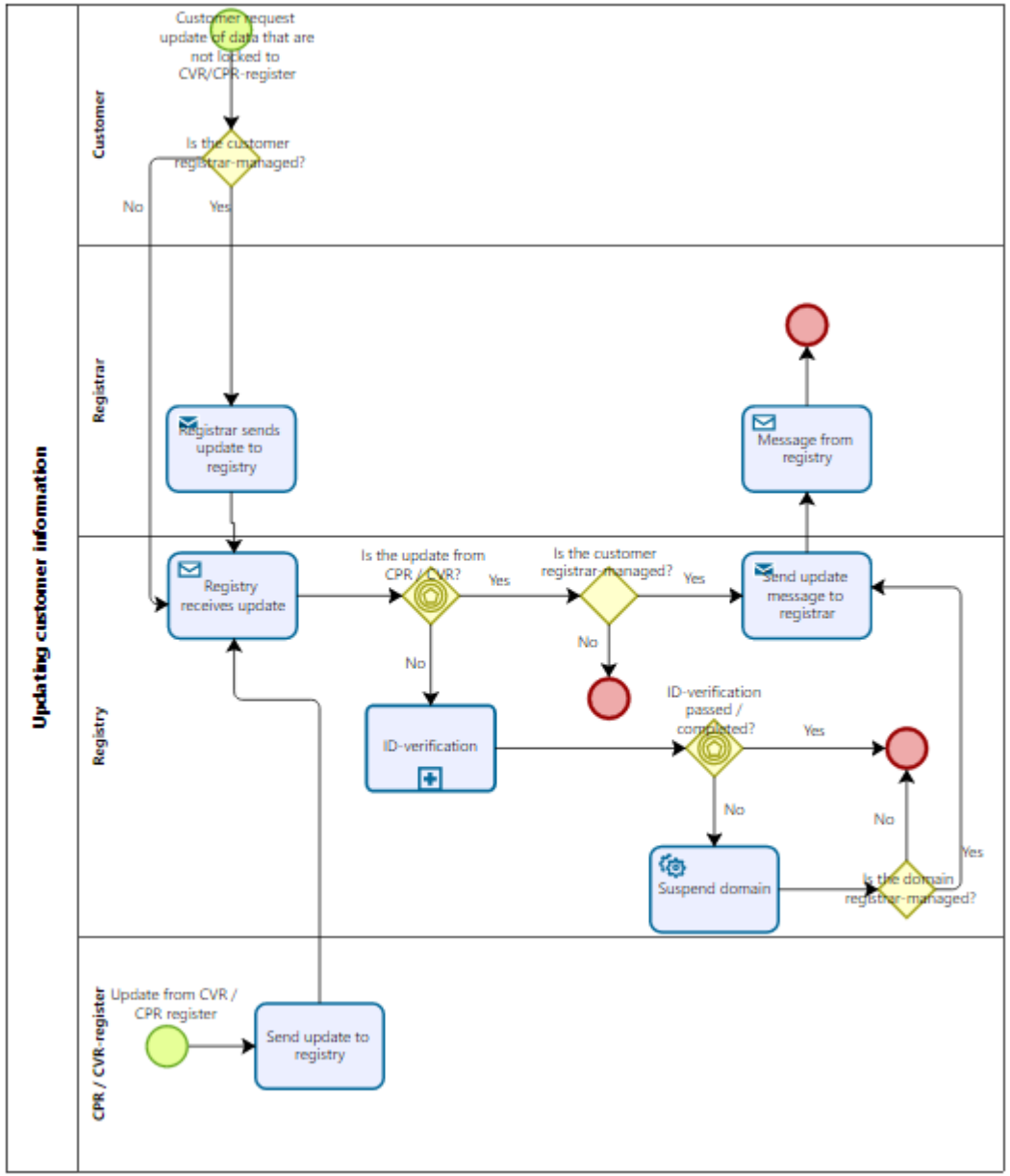
Detailed flow chart (1)

Overview of *collecting*
domain name registration data



Detailed flow chart (2)

Overview of *maintaining*
domain name registration data



Solution on ensuring correct and complete Domain Name Registration Data (2)

Main principles

- The model shall provide registrars with flexibility in complying with NIS2, Article 28
- A hybrid model is introduced where registrars can choose, if the registrar verifies data or the verification is done by Punktum dk
- For verification methods see document "approved verification methods" (Appendix 1)

What data is verified

Registrant

- Name
- Address
- Phone number
- Email

Point of Contact (proxy)

- Phone number
- Email

When is data verified

Domain name registration data is verified (incl. risk assessment)

- When a user becomes registrant (It can happen at registration and if a registrant transfers a domain name to a new registrant)
- When a user becomes point of contact (proxy)
- When user data is updated*
- Ad hoc e.g. if data seems suspicious
- If Punktum dk receives a well-founded report that registration data in WHOIS is not accurate based on section 15 of the executive order on the internet domain .dk (§15-reports)

**if the registrant has address in Denmark and data is locked to CPR/CVR a separate verification is not necessary*

Who verifies a new user – Hybrid model (1)

Registrar can choose if verification is done by registry or registrar:

- The option is set in the registrar's profile > the registrar choose, if the registrar wants to verify data ("registrar verification") or the registrar want the registry to do the verification ("registry verification")

Before creation of a user

- Registrar can always verify user data no matter profile setting
  - Domain registration will be activated without further control

After creation of a user

- If the user is managed by the registrar > the verification will be done by registrar, if verification is necessary and "registrar verification" has been chosen > If so, registrar will be notified by registry
- If the user is managed by the registrar > the verification will be done by registry, if verification is necessary and "registry verification" has been chosen
- If user is managed by the registry > the verification will be done by registry, if verification is necessary.

Who verifies updated user data for DK resident – Hybrid model (2)

Verification of updated user data for DK resident by registrar is only relevant, if the user is managed by the registrar:

- DK resident will be locked to CPR/CVR > Registry sends updated name and address from CPR/CVR to registrar.
  Exemption: Users with name and address protected from publication is not locked to CPR > Registrar sends updated address to registry
- Registrar updates email and phone number > Registrar sends updated email and phone number to registry

If updated data has already been verified:

- Registrar can specify that updated user data has been verified

If user data has not been verified before update of user data:

- Registrars profile setting determines whether the registrar or registry makes the verification of data

Registrant is managed by registrar	Updated data	Verification status	Who does the verification
	Name and address	Locked to CPR/CVR	Updated information is sent from registry to registrar – no need for verification
	Phone and email (+ address if not locked to CVR/CPR)	Not locked	Registrar makes verification, it the registrar has chosen "registrar verification"
			Registry makes verification, if the registrar has chosen "registry verification"

Who verifies updated user data for non-DK resident – hybrid model (3)

Registrar updates user data (address, email and phone number) if the registrant is managed by the registrar > registrar sends updated user data to registry. Only registry can update name (see slide 15).

If updated data has already been verified:

- Registrar can specify that updated user data has been verified
  - Note: If only some of the user data is updated, e.g. a phone number the update of user information will trigger a risk assessment of all user data, when user is resident outside of DK. This is due to change of one data set, can influence a former risk assessment.

If user data has not been verified before update of user data:

- Registrars profile setting determines whether the registrar or registry makes the verification of data, if risk assessment triggers a verification request

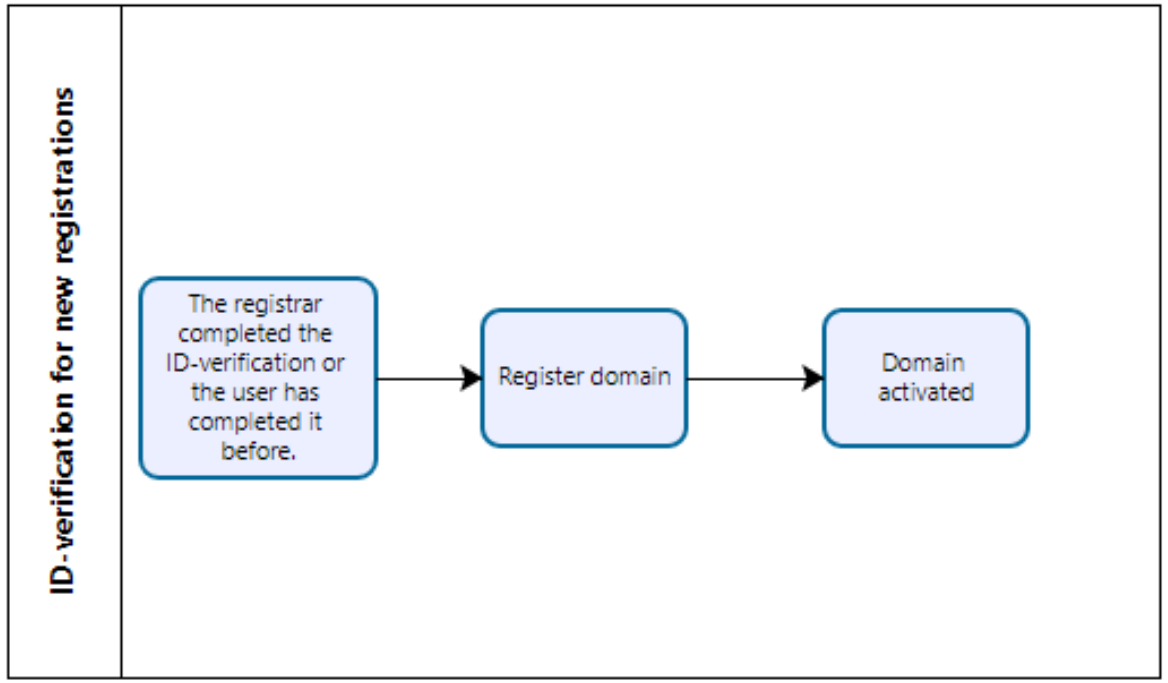
Registrant is managed by registrar	Updated data	Verification	Who does the verification
	Address, phone number and email	Data has already been verified > No need for verification	Updated information is sent from registrar to registry
		Data has not been verified > risk assessment can trigger a new verification request	Registrar makes verification, it the registrar has chosen "registrar verification"
			Registry makes verification, if the registrar has chosen "registry verification"

Registration of a domain name

Scenario 1: Registrant data has previously been verified

Process for new registration of a domain name:

- Registrar can check registry's system, if the registrant's data has already been verified (registrant already has a handle)
- Registrar can also choose to complete verification before domain name is created
- Registrar sends a domain registration request to registry
- Domain is created
- Domain name is activated

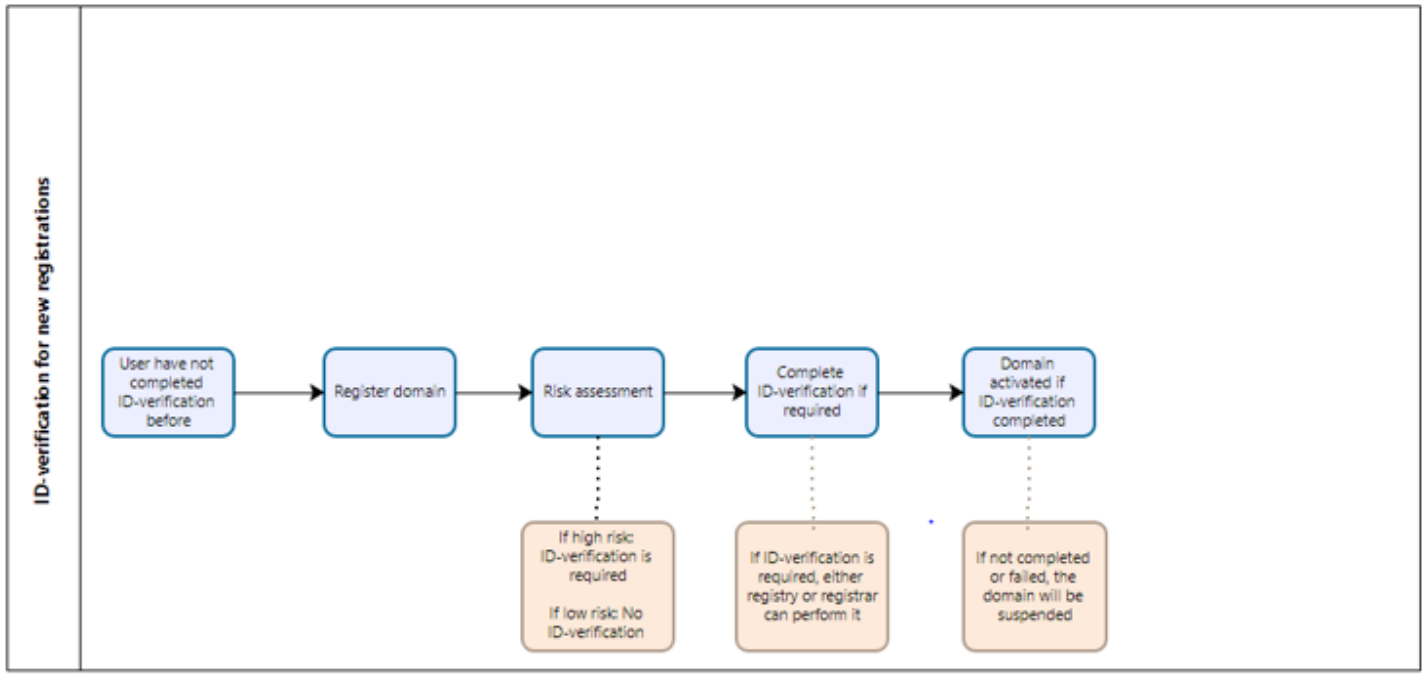


Registration of a domain name

Scenario 2: Registrant data has *not* previously been verified

Process for new registration of a domain name:

- User has been created (see process slide 16)
- Domain name is created
- Non-DK resident
  Risk assessment is completed by Punktum dk
- DK-resident
  Verification is mandatory
- If verification is required, registrar can choose if registry or registrar do the verification
- Domain name is activated, if verification is completed
- Domain name is suspended, if verification is not completed within 30 days

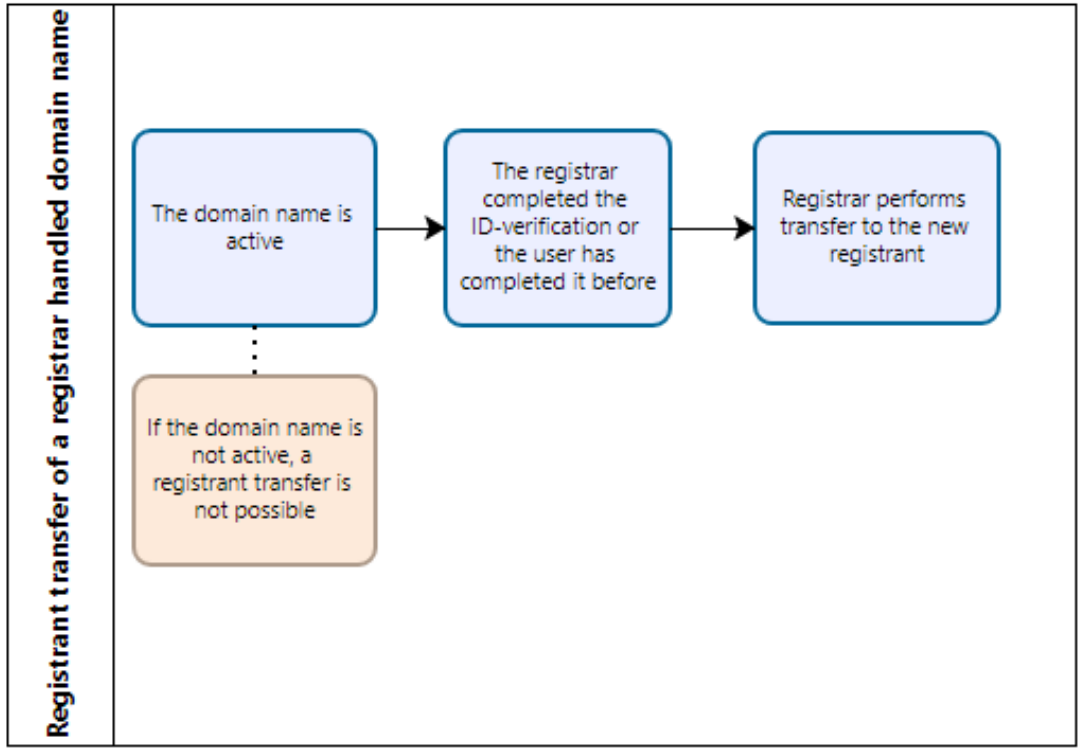


Registrant transfer of a domain name

Scenario 1: New registrant's data has previously been verified

Process for registrant transfer:

- Domain name is active
- Registrar can check registry's system, if the new registrant has already been verified (registrant already has a handle)
- Registrar can choose to complete verification before domain name is transferred
- Registrar performs transfer to new registrant

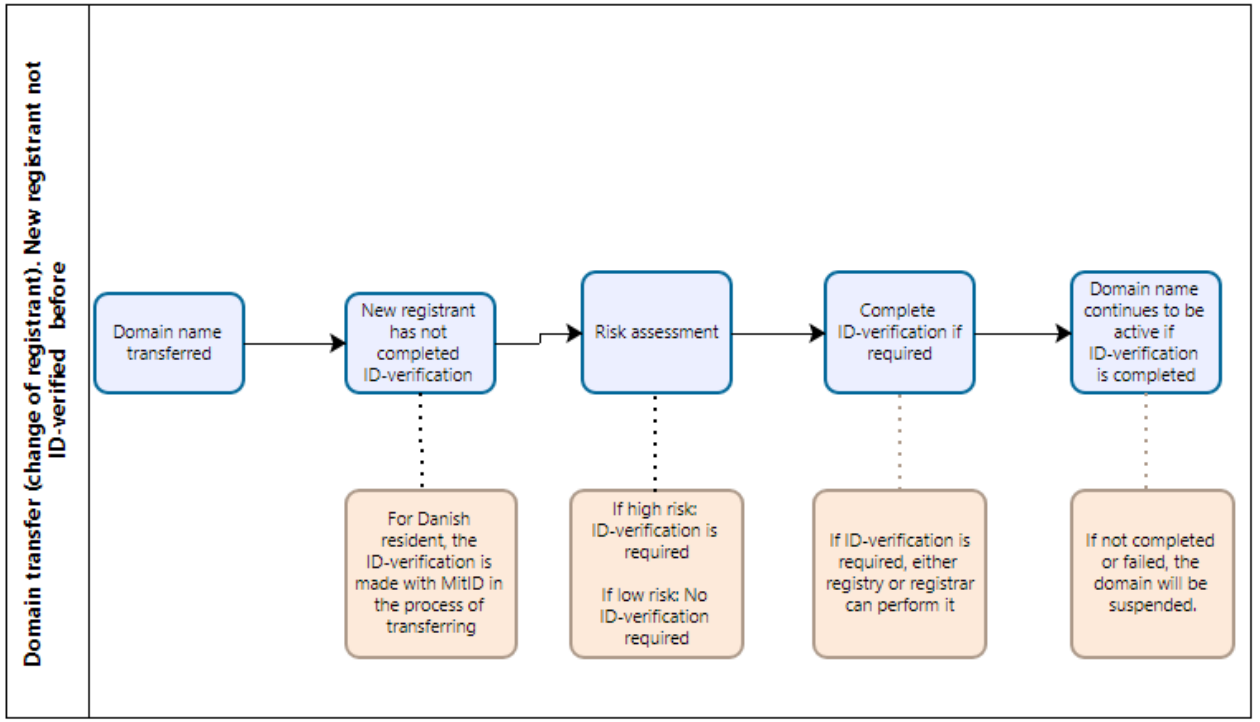


Registrant transfer of a domain name

Scenario 2: If new registrant's data has *not* previously been verified

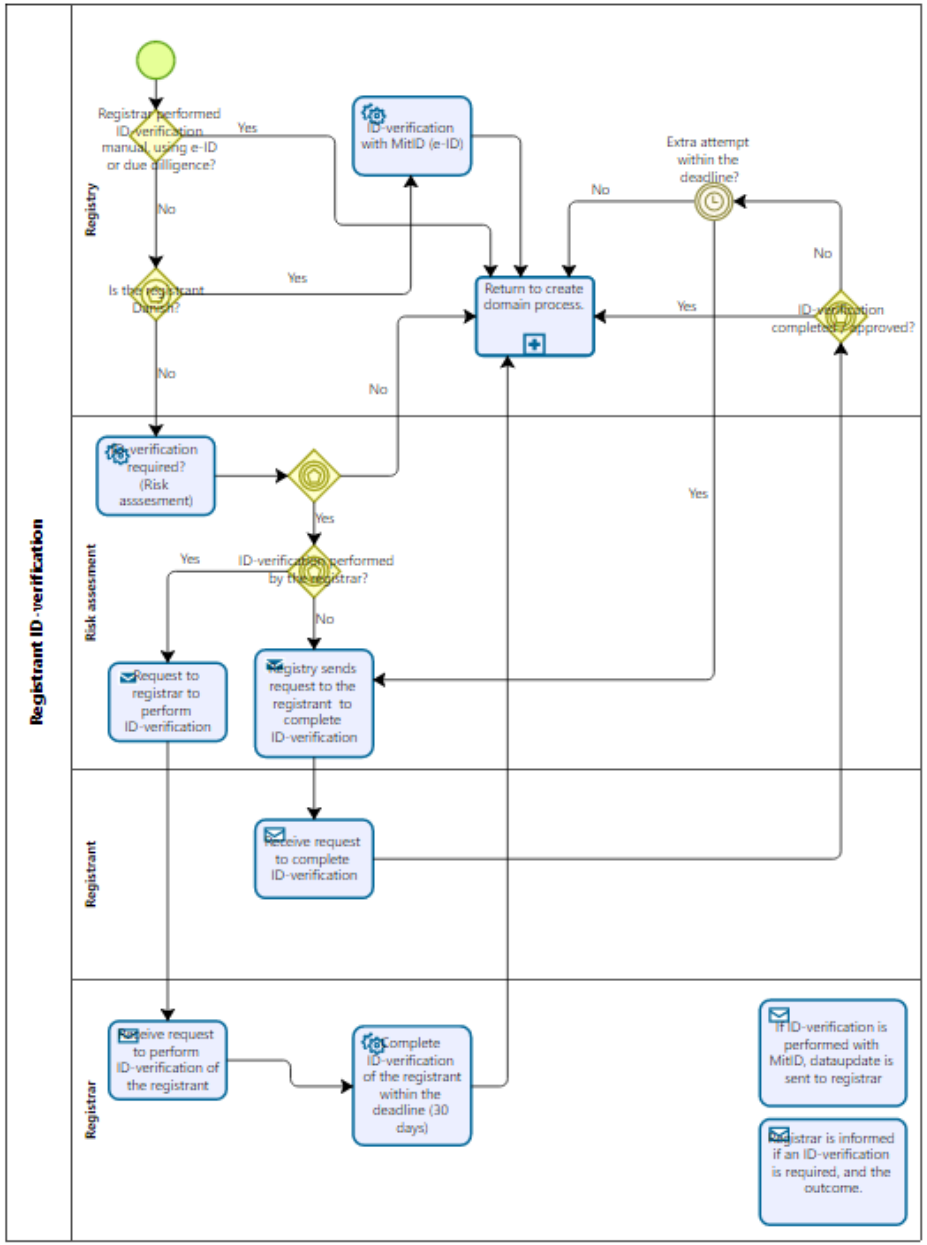
Process for registrant transfer:

- Domain name is active
- New registrant has not been verified before
- DK resident > MitID-control
- Non-DK resident > Risk assessment is completed by Punktum dk
- If verification is required, registry or registrar can perform the verification
- Domain name is suspended, if verification is not completed within 30 days



Detailed flow chart

Overview verification of data
(Verification process)



Publication of Domain Name Registration Data (3)

Main principles

According to NIS2, article 28, domain name registration data which are not personal data must be made publicly available with undue delay after registration of a domain name. The Domain Act requires Punktum dk to publish name, address and phone number of a registrant also if it is personal data.

- Punktum dk's will publish data according to NIS2 and the Domain Act in the public WHOIS on Punktum dk's website

Due to the legislation a distinction must be made between a private and legal person and for legal persons between personal and non personal data.

What data is published for natural persons

Published according to NIS2 and Danish Domain Act

Domain name

- Date of registration (created)

Registrant

- Name
- Address
- Phone number

Point of Contact (proxy)

- If private person, data will not be published

What data is published for legal persons

Published according to NIS2 and Danish Domain Act

Domain name
- Date of registration (created)

Registrant
- Name
- Address
- Phone number
- Email - unless it contains personal data

Point of Contact (proxy)
- Phone number
- Email - unless it contains personal data

Other information that is published

Punktum dk will also, as today, publish on its website:

- Domain name status
- Name server
- Contract information on registrar if domain name is managed by registrar

Following other technical data will be available elsewhere:

- DNSSEC
- VID service
- Delete date

Categorisation of e-mail

- Legal person and private person are distinguished based on the information provided by the user when user is created, or data is updated
- Parties must ensure assignment of correct type of person (Legal/natural)
- Parties must ensure that legal persons are effectively informed that email must not contain personal data and data will be published

Technical solution on how to share necessary data (4)

(See Appendix 2)

Compliance and audit (5)

Compliance and audit – Framework Conditions

- Verification obligations resulting from NIS2 will be included in an Allonge to the registrar agreement, making "verification by registrars" possible
- Punktum dk can audit registrars' compliance with the Allonge > can require documentation for verifications completed within the last 30 days.
- Audit will include documentation in relation to approved verification. See next slide for what this can include
- The existing registrar agreement regulates non-compliance with the requirements for "verification by registrars"

Use of third parties to do verifications

- The registrar can use 3. parties, incl. resellers, to do the verification
- If so, the registrar must still ensure that the verifications comply with the requirements in the registrar agreement with Punktum dk
- Registrar sends necessary documentation to Punktum dk upon request

Documentation for audit

Following documentation can be relevant for Punktum dk to request from registrar in connection with an audit:

E-ID	Pre-approved in-depth onboarding process	Documentation received	Email (active response)	Phone number
Log file, containing the single transaction with the e-ID used. If address is in the e-ID this must be included in the log file	Documents and video identification, if video is used corresponding to the approved process	Documents and video identification, if video is used	Confirmation from registrant. Depending on method use, it can be a confirmation e-mail and log file. Always with timestamp and date combined with the e-mail sent to the registrant	Procedure for syntax check and ad hoc check, e.g. if data seems suspicious

Approved verification methods

NIS2, Article 28

Terminology

Natural registrant
A human being/physical person

Legal registrant
A legal entity that has rights and duties just like a natural person. The term typically covers companies and organisations, but also states, municipalities and other public institutions

Active response
The registrant actively confirms that he/she has access to the e-mail address and/or telephone number, e.g. access something through a link sent to the e-mail address or by SMS to the phone number

Passive response
The registrant passively confirms that data is accurate and up-to-date. It can be via a notification on self-service portal when user logs in or an e-mail to user that the user must react if the data is no longer accurate

Natural registrant resident in Denmark

Identity	Address
• MitID	• MitID (includes address)

Note
Will be locked to CPR (Central Personal Register) and data is automatically updated Exemption: if a person's name and address is protected from publication

Legal registrant resident in Denmark

Identity	Address
• MitID	• MitID (includes address)

Note
Will be locked to CVR (Central Business Register) - data is automatically updated

Natural registrant resident outside Denmark

Identity	Address
• eID without address • Passport with picture • National drivers license with picture • National identity card with picture • Bank transfer to the registrar matching the domain holder's name • Video Identification (3. parties offers video of registrant with passport/ID-card)	• eID with address • Document from a utility company (gas, electricity, water, internet or phone) • Bank statement • Invoice rent or rental agreement • Document from insurance company
Conditions	**Conditions**
• Must carry registrant's name • Must correspond to name already registered • Must be combined with a recent selfie (except with eID and Video Identification)	• Max 3 months old • Must carry the registrants name and address • Must correspond to name and address already registered

Legal registrant resident outside Denmark

Identity	Address
• eID • Two types of documentation from a public authority (company register, tax authority, VIES). One which is not publicly available * (next slides will elaborate on this) • Bank transfer to the registrar matching the domain holder's (not a money transfer like WISE, Western Union) • Documentation from a company register combined with identification of a natural person (by a method described under "Identification of a natural person resident outside Denmark or by notary) who is authorized to act on behalf of the company according to the company documentation • Pre-approved in-depth onboarding process	• eID with address • Document from a utility company (gas, electricity, water, internet or phone) • Bank statement • Invoice rent or rental agreement • Documentation from a public authority with address (company register, tax authority, VIES) • Pre-approved in-depth onboarding process
Conditions	**Conditions**
• Must carry the company's name • Must correspond to name already registered	• Max 3 months old • Must carry the company's name and address • Must correspond to name and address already registered

If documentation fulfils the requirement for both identity and address the same document can be used to verify both identity and address

Examples documents from a public authority

- Documentation from a tax authority, e.g. tax certificate
- Documentation from a Business Register, e.g. business certificate
- Letter from a public authority
- Permit and licenses issued to the company from a public authority e.g. to operate in certain industries or locations
- Trademark Registration Certificate
- Health and Safety Inspections Reports
- Invoice from a public authority

Examples documents from a public authority that might not be public available

- Documentation from a tax authority, e.g. tax certificate
- Documentation from a Business Register, e.g. business certificate with signature and stamp from the Business Register
- Letter from a public authority
- Permit and licenses issued to the company from a public authority e.g. to operate in certain industries or locations
- Invoice from a public authority

- Parties must make a concrete assessment of the documentation

Registrant

Phone number	E-mail Address
• Syntax check* OR Active response AND • Well-founded report to that registration data in WHOIS is not accurate (§ 15-reports) • Ad hoc e.g. if data seems suspicious • Can be combined with passive response, e.g. when login to self-service-portal	• Active response
Note	**Note**
• Both at registration and updating of phone number (* Authorities has not yet decided if this will be enough or active response will be necessary)	• Both at registration and updating of e-mail address • Can be part of established processes, e.g. when email is sent to registrant to complete verification

NIS2, Article 28, Technical Working Group Solutions

General Principles

- Registrar can freely choose if they will be responsible for the verification or registry should handle it
- There will be a 30 day time limit for completing the verification at which point domains are suspended. This applies to both registrar and registry handled verifications
- Email bounces detected by registry **will not trigger a verification process**
- If registrar detects email bounces, registrar is required to provide updated contact email information to registry
- If registrar detect contact information on already verified contacts not being correct, registrar is required to provide updated contact information to registry. **No new verification is required by registry**
- Registry will ensure complete and timely notification of any status changes on ongoing verifications

Feature List

Punktum dk Registrar Portal

- Enable registrar to define default verification scheme, registrar or registry (default) on their account in the Registrar Portal
- Enable registrar to specify on contact creation form, if verification has been completed
- Enable registrar to update registrar handled contact if verification is completed after creation
- Enable registrar to get an overview of all pending verifications on registrar handled contacts
- Enable registrar to see current verification status of individual registrar handled contacts

Punktum dk EPP

- Add extension to indicate if verification has been completed on contact (true/false) og both create and update commands
- Add extension to indicate status of pending verifications including expire date on registrar handled contacts
- Add poll messages regarding status changes on pending verifications handled by registry

Note: If Danish contacts cannot be locked to CPR/CVR registries verification process is started by registry regardless of status set by registrar

Feature List (continued)

Punktum dk Self-Service Portal

- Non-private users should be clearly informed, that email addresses will be public and must not contain personal information
- *Registrars must ensure similar feature in their own platforms*

Notifications

- Registrars not using EPP will receive all messages offered in poll as email instead. Feature to configure general account notification settings is being address in another initiative