

The Cybersecurity Act Netherlands - Cyberbeveiligingswet (CbW) provisions related to domain name registration data

Entity	SIDN ^{1,2} , Gemeente Amsterdam ³ , Dotlocal	Registrars based in the Netherlands ⁴
TLD's	.nl / .amsterdam / .frl ⁵	All TLD's
Cbw Provision		
(1) Collection of accurate and complete domain name registration data (Art. 49 sub 1 CbW)	1. At least the minimum data as described in art. 49 sub 2 CbW must before the registration of a domain name be collected by the registrar. 2. The registrar must register a domain name at the registry with at least the complete minimum data. 3. The registrar must in the registration process provide at least the minimum data to the registry.	1. At least the minimum data as described in art. 49 sub 2 CbW must before the registration of a domain name be collected by the registrar. 2. The registrar must register a domain name at the registry with at least the complete minimum data.⁶ 3. The registrar must in the registration process provide at least the minimum data to the registry.
(2) Requirements for database of domain name registration data (Art. 49 sub 2 CbW)	1. Data collected via the registrars is at the minimum the set as mentioned in art. 49 sub 2 CbW.	1. Data collected via the registrars is at the minimum the set as mentioned in art. 49 sub 2 CbW

¹ SIDN is also the backend registry provider for .aw (the ccTLD for Aruba). The registry for .aw is SETAR, an Aruba based entity which offers the .aw only locally. .aw does not fall under the scope of the CbW.

² SIDN is also the backend registry provider for .politie. The registry for .politie is the Nationale Politie. The .politie-domain is still in its pre-launch state. Currently only the Nationale Politie has the ability to register a limited number of domains for its own use. In the current state .politie does not fall under the scope of the CbW.

³ The Gemeente Amsterdam is the registry for .amsterdam. The Gemeente Amsterdam has outsourced all registry operations to Dotlocal which has outsourced the technical backend registry to SIDN.

⁴ In line with article 4 sub 4/5 CbW these are all registrars that have their main establishment in the Netherlands or, if based outside of the EU, those registrars that have appointed a representant based in the Netherlands.

⁵ The registries for these TLD's will implement these obligations through their contracts with their registrars.

⁶ Some registries only accept for TLD's less than the minimum data set (thin gTLD-registries and some ccTLD's). The minimum data will however in all cases be kept by and be available at the registrar. {note: ask Maarten for clarifications to improve the readability of the text.

(3) Verification of domain name registration data (Art. 49 sub 3 CbW)	1. The registrar must upon every new registration, transfer, or update verify that the email address or phone number on file has been verified conform the verification procedure as provided for by ICANN⁸ to verify the registration data. 2. The registrar must wait for the successful outcome of the email verification procedure before activating the domain name for the registrant for a newly registered domain. 3. The registrar must at least annually in line with ICANN's Registration Data Reminder Policy⁹ present to the registrant the actual registration data, remind the registrant of its obligation to keep this data correct and urge the registrant to update the data if it is incorrect. 4. The registry must verify the identity of a registrant via an (e)ID-check if it has reasons to believe that the registered registrant details may be incorrect. Such reasons may for example be based upon notices from third parties or risk assessment systems used by the registry. 5. The registry must publish on its website its policies and procedures in place to assure the correctness and completeness of its TLD's registration data.	1. The registrar must upon every new registration, transfer, or update verify that the email address or phone number on file has been verified conform the verification procedure as provided for by ICANN⁸ to verify the registration data. 2. The registrar must wait for the successful outcome of the email verification procedure before activating the domain name for the registrant for a newly registered domain. The registrar must at least annually in line with ICANN's Registration Data Reminder Policy⁹ present to the registrant the actual registration data, remind the registrant of its obligation to keep this data correct and urge the registrant to update the data if it is incorrect. 4. The registrar must re-verify previously verified registration data if it has reasons to believe that this data has become incorrect. If such re-verification fails, registrar shall either verify the data manually or (temporarily) suspend the registration. 3. The registrar must publish on its website its policies and procedures in place to assure the correctness and completeness of the registration data for the domains under its management.
(4) Publication of domain name registration data (Art. 49 sub 4 CbW)	1. The registry must provide a domain name look up service on its website that is open for all internet users and provides upon request at the minimum for each domain in the TLD the minimum data as described in art. 49 sub 2 CbW as far as this data is not personal data.	1. The registrar will, at least if a registry for a TLD does not already provide such service provide a domain name look up service on its website that is open for all internet users and provides upon request at the minimum for the domains under their management the minimum data as described in art. 49 sub 2 CbW as far as this data is not personal data.
(5) Non-duplication principle (Art.49 sub 5 CbW)	1. Collection (directly or via a reseller or other third party) and other processing activities related to domain name registration data are carried out only by registrars.	1. All registration data must only be collected by the registrar (directly or via a reseller or other third party).

(6) Access to domain name registration data (Art. 50 sub 1 CbW)	1. The registry must provide at its website information for legitimate access seekers how to request for a domain registration data that is not publicly available via its domain registration look up service. This may be via a webform or an email address.	1. The registrar must provide at its website information for legitimate access seekers how to request for a domain registration data that is not publicly available via its domain registration look up service. This may be via a webform or an email address.
(7) Timelines for access to domain name registration data (Art.50 sub 2 CbW)	1. The registry must have procedures in place to evaluate such requests and must respond without delay but at the latest within 72 hours upon the reception of such a request.	2. The registrar must have procedures in place to evaluate such requests and must respond without delay but at the latest within 72 hours upon the reception of such a request.
(8) Timelines for access to domain name registration data (Art.50 sub 3 CbW)	1. Registries must make publicly available (on their website) policies and procedures related to requesting access to non-public registration data.	1. Registrars must make publicly available (on their website) policies and procedures related to requesting access to non-public registration data.