Questions with clarifications after NIS2 registrar meeting October 22th, 2025

Nr	NIS2 questions	Conclusion	Decisions from NIS2 working group
1	Do verification requirements allow registrars to verify only certain fields of a registrant's information?	**Registrar responsibilities in registrant verification** **Comprehensive data verification:** The registrar is required to verify all essential contact data points: the registrant's name, address, and email address. **Verification status requirement**: The verification status can only be set to "Verified" if all mandated data fields — name, address, and email — have been successfully verified. Partial verification is **not** sufficient. **Optional pre-verification:** If the registrar chooses to verify only Danish registrants (DK registrants) or non-Danish registrants (non-DK registrants), this data verification can be performed proactively before the end-user account is formally created. **Streamlined user experience:** To prevent confusion and friction, the registrant will receive verification requests from only one entity: either Punktum dk or their chosen registrar. The systems are designed to ensure the user – as a main rule – is not subjected to duplicate requests (see question 2 below).	Decision from the 7th meeting, where "all-or-nothing model" was agreed to make the process as easy as possible: "There was a discussion about the slide "Implementation Hybrid Model. [...] If a registrar chooses not to do the verification for all registrants, the registrar can still do the verification up front and flag that verification has been done. In these cases, Punktum dk will not do the verification as it has already been done. There was an overall wish from registrars to keep it as simple as possible so a registrar can choose to do or not to do all the verification (for all users and all data) or choose not to do any of the verification." Punktum dk informed in the 12th meeting : "However, it has become clear that it is technically not possible to have only one data point to handle registration of whether identity and contact information of the registrant has been verified. This implementation will therefore consist of three separate data points to signal state of verification: one for identity and postal address, one for email and one for telephone numbers. It is still an all-or-nothing solution as agreed upon so that all three data points must be marked as completed for registrant verification, for proxies only the data points concerning email and telephone number."

2	Does Punktum dk still conduct registrant data verification even if the registrar has already verified the information upfront?	**Punktum dk will normally not verify the registrant's data, if the registrar has already done it.** **Non-DK registrant:** If the registrar marks the registrant has been verified, Punktum dk will accept the registrar's verification and will not override registrars' verification. (See question 3 below about risk assessment). **DK-registrant:** Punktum dk is legally obliged under Danish domain law to ensure the highest degree of registrant data accuracy. To comply with this mandate, we will always attempt to link (lock) a registrant's identity to either the official Central Person Register (CPR) or the Central Business Register (CVR). This locking mechanism is crucial as it guarantees data quality and automatically provides us with timely updates regarding changes in name, address, or legal status for both private individuals and legal entities. In cases where it is **not** possible to lock the registrant, Punktum dk will start a verification of data.	If the submitted data is accurate, it should be possible to link a DK-registrant to the Central Person Register (CPR) or Central Business Register (CVR). However, in certain cases, discrepancies between the submitted data and the CPR or CVR registers may prevent this linkage. In such instances, Punktum DK will verify the registrant. To reduce the likelihood of discrepancies and improve the accuracy of submitted data, registrars may consider implementing address lookup features, noting that Danish addresses can be accessed free of charge from public registries. Main document, annex 2: "If Danish contacts cannot be locked to CPR/CVR registries verification process is started by registry regardless of status set by registrar"

3	If a registrar uses the EPP/RP to confirm a new contact as already verified, will Punktum dk subsequently perform a risk assessment that automatically could trigger a second, mandatory verification for that same registrant?	**Punktum dk registrant data verification policy** The primary goal is to ensure registrants only need to complete the data verification process once. **During contact creation (initial verification)** **Non-DK registrants (Marked verified):** If the registrar marks a non-DK registrant as already verified upon creation, Punktum dk will not initiate a new risk assessment or request further verification. This ensures the domain name is entered into the zone without delay. **DK Registrants (Marked verified):** If the registrar marks a DK registrant as verified upon creation, Punktum dk will only request new verification if the registrant data cannot be successfully matched the Central Person Register (CPR) or Central Business Register (CVR). **Post-Creation verification and renewal** **Unverified data:** If the registrar explicitly marks the registrant's data as NOT verified, Punktum dk will perform a post-creation risk assessment. This assessment may result in a formal request for the registrant to complete verification. **Domain renewal (NIS2 requirement):** In compliance with the NIS2 executive order, Punktum dk is required to perform a new risk assessment on non-DK registrants upon the renewal of every domain name. The registry's standard risk assessment methodology will be applied at this stage.	Agreed upon at the 4th meeting that Punktum dk should make the risk assessment: "*...stated, that the risk assessment could continue to be made by Punktum dk to get a uniformly risk assessment and that the actual verification then could be made by the registrar, if so wished.* *[...]* *...agreed that the risk assessment could be done by the registry and stretched the need for flexibility concerning the methods for verification.* *[...]* *It was agreed that Punktum dk should make the risk assessment.*"
4	When does the registrant's email need to be verified?	**Email address confirmation requirement:** To ensure the new email address is both correct and actively monitored by the registrant, Punktum dk requires active confirmation of the email address whenever it is: **1. Registered:** During the initial domain registration process. **2. Updated:** Whenever the email address associated with the registrant contact is modified.	Main document, annex 1: Approved verification methods: page 9. Active response of an e-mail address must be done "*both at registration and updating of an e-mail address*".

5	Does Punktum dk verify primary or secondary e-mail address?	**Both emails are validated** (separately) when they are entered or updated but there is no requirement that you have two emails. **However,** there is a requirement that the email that is published must not contain personal data. If an email is entered in the secondary email, it will be published. If not, the primary email will be published. **NOTE**: Only company emails will be published (excluding sole proprietorships)	
6	Why does Punktum dk require mandatory CVR/CPR lock for Danish registrants, and what are the risks of relying solely on the data supplied by registrars?	**Rationale for Punktum dk's registrant data policy** **Legal mandate for verification:** Punktum dk is legally required under Danish Domain Law to tie Danish domain registrants to the official state registers. This necessity drives the implementation of mandatory linkage to the Central Person Register (CPR) or Central Business Register (CVR). **Ensuring data integrity and automation:** Punktum dk automatically maintains and updates the name and address details for all registrants residing in Denmark ("DK registrants"). This real-time accuracy is achieved by locking registrant information directly to the Central Person Register (CPR) or Central Business Register (CVR). **Upholding privacy protections:** Furthermore, the linkage to the CPR system is crucial for complying with privacy requirements mandated by Danish Domain Law. By cross-referencing with the CPR, Punktum dk ensures that the addresses of registrants who have activated name and address protection within the Danish Civil Registration System are withheld from public WHOIS records.	Agreed upon at the 3rd meeting: *"The working group agreed following at its last meeting in relation to collection of up-to-date data information:* *1.Domain name is handled by the registrar = the registrar collects updated information.* *2.Domain name is handled by the registrant = .dk collects updated information.* *It was discussed whether there should be an exception to nr. 1 regarding name and address. The reason for this is that Punktum dk today updates name and address on all registrants residing in Denmark ("DK registrant") automatically. This can be done by locking registrants towards the Danish CPR and CVR registers.* *Punktum dk also locks DK registrants towards CPR to ensure that addresses are not made public in WHOIS, if a registrant is registered in the Danish Civil Registration System as having name and address protection. This is a requirement according to the Danish Domain Law.* *Exceptions for the collection of updated information.* *It was agreed:* *If it is possible to change the Danish Domain Law, whereas the registrants address is excluded or should not be automatically protected (made anonymous) when possible, there should be no exemption to nr. 1 - meaning the registrar always collects updated information* *If it is not possible to change the Danish Domain Law – DK registrants will be locked towards CPR and CVR by Punktum dk as it is done today."*