

The RIPE NCC membership consists of parties from various industries and countries. We recognise that some of our members may be subject to DORA, and therefore we strive to address their needs to the best of our ability. While the DORA requirements apply to financial institutions, the RIPE NCC aims to facilitate to a reasonable extent the implementation of this regulation for those entities that are RIPE NCC members.

After a careful analysis of the DORA provisions in relation to our services, we have concluded that relevant requirements may be addressed by amending the legal framework for the LIR Portal (LIR Account Agreement), RPKI services (Certification Service Terms and Conditions, Publish in Parent Service Terms and Conditions and Certification Repository Terms and Conditions) and RIPE Database (RIPE Database Terms and Conditions), all together further referred to as the 'Legal Framework'.

Please find below the overview of how we facilitated the implementation of each provision mentioned in article 30.2 of DORA in our Legal Framework:

30.2a Functions, ICT services and subcontractors:

- i. A description of our services is included in the respective terms and conditions of our RPKI services as well as the RIPE Database and the LIR Account Agreement.
- ii. The list of subcontractors for each service is published in the Trust Portal (https://www-static.ripe.net/static/ripencc_26/20260126_The_RIPE_NCC_DORA_Whitepaper_registry.pdf) as described in the relevant provisions of the Legal Framework:
 - Article 8.4 of the LIR Account Agreement
 - Article 7.5 of the Certification Service Terms and Conditions
 - Article 8.5 of the Publish in Parent Service Terms and Conditions
 - Article 6.4 of the Certification Repository Terms and Conditions
 - Article 8.4 of the RIPE Database Terms and Conditions

30.2b Locations of functions, services and data storage

The locations of our services (falling under DORA), data storage and our subcontractors' services and data storage are published in the Trust Portal (https://www-static.ripe.net/static/ripencc_26/20260126_The_RIPE_NCC_DORA_Whitepaper_registry.pdf)

The above-mentioned provisions of the Legal Framework refer to this list.

With regards to notifying members in advance about changes in the location of subcontractors' data storage, as we are not necessarily notified by our subcontractors of such changes on time, we cannot commit to notifying our members of them either.

30.2c Availability, authenticity, integrity and confidentiality

This is addressed in the [RIPE NCC Privacy Statement](#), [Data Protection Report](#), the [Database Acceptable Use Policy](#) as well as in the Security Information published in the Trust Portal (<https://trust.ripe.net/information-security/security-policies/>). The relevant provisions in our Legal Framework are the following:

- Article 8.6 of the LIR Account Agreement
- Article 7.7 of the Certification Service Terms and Conditions
- Article 8.7 of the Publish in Parent Service Terms and Conditions
- Article 6.6 of the Certification Repository Terms and Conditions
- Article 8.6 of the RIPE Database Terms and Conditions

30.2d Insolvency, resolution or discontinuation of the business operations

The services addressed by DORA are related to the function of the RIPE NCC as a Regional Internet Registry (RIR). The criteria of establishment and operation of an RIR are currently described in the document “Internet Coordination Policy 2” (ICP-2). The global Internet community is now in the process of revising this document and is working on a new document with an extended scope that includes the derecognition of an RIR and the relevant consequences (please see: <https://www.ripe.net/community/nro-nc/icp-2-review/>).

As the matter of discontinuation will be addressed by this revised document, any relevant amendments to the Legal Framework may be implemented upon its adoption.

30.2e Service Levels

Currently, there is no available service level information. However, should this become available, all information will be published in the Trust Portal as per the following articles in the Legal Framework:

- Article 8.5 of the LIR Account Agreement
- Article 7.6 of the Certification Service Terms and Conditions
- Article 8.6 of the Publish in Parent Service Terms and Conditions
- Article 6.5 of the Certification Repository Terms and Conditions
- Article 8.5 of the RIPE Database Terms and Conditions

30.2f Assistance in case of ICT incidents

The RIPE NCC provides assistance during ICT incidents through the Technical Emergency Hotline (<https://www.ripe.net/about-us/support/contact/technical-emergency-hotline/>). Any information about a confirmed ICT incident can be found on the Services Announcement page (<https://status.ripe.net>) as described in the following provisions of the Legal Framework:

- Articles 4.2 and 4.3 of the LIR Account Agreement
- Articles 4.4 and 4.5 of the Certification Service Terms and Conditions
- Article 6.2 and 6.3 of the Publish in Parent Service Terms and Conditions
- Article 4.2 and 4.3 of the Certification Repository Terms and Conditions
- Articles 5.6 and 5.7 of the RIPE Database Terms and Conditions

30.2g Cooperation with competent authorities of members

The RIPE NCC commits to complying with legally binding orders by Law Enforcement Authorities.

More information on our cooperation with Law Enforcement Authorities can be found here: <https://trust.ripe.net/law-enforcement-and-competent-authorities/>.

30.2h Termination of the agreement

The termination of an LIR Account Agreement is defined in article 6 of the agreement. The RIPE Database Terms and Conditions and the Certification Repository Terms and Conditions do not have a termination clause because they are public services. Users may cease using these services at any time.

A provision regarding termination of the Certification Service can be found in article 5.1 of the relevant Terms and Conditions.

30.2i Security awareness programmes and digital operational resilience training

All of the RIPE NCC's employees receive comprehensive security awareness training during their onboarding phase and at least annually thereafter. The topics of the training include data protection, phishing prevention, secure password management and compliance with company security policies to mitigate cybersecurity risks, among others. More information on organisational security can be found here:

<https://trust.ripe.net/information-security/organisational-security/>

Given the large number of our members, a commitment to participate in all members'/users' security awareness programmes and digital resilience training is not pragmatic. Therefore, such a commitment is not addressed in the Legal Framework.

Should you have any questions, you may contact us via ncc@ripe.net.