.DE Domain Risk Assessment and Identity Verification Process

Overview

DENIC (the .DE registry) introduces **automated risk assessment** for:

- New registrations
- Transfers
- Owner changes
- Contact updates

The registry evaluates the **domain holder’s name and address**. If flagged, identity verification is required.

---

1. What’s Changing

Previously, checks were manual. Now, DENIC uses an **automated algorithm**.

Evaluated data:

- Holder name
- Holder address
- Individual vs organization

If data looks suspicious:

- DENIC → sends poll message
- Openprovider → emails reseller

---

2. Risk Levels

Low Risk

- Domain works normally, and no action is needed.

Suspicious

- Domain works normally, verification required within **30 days**

If not completed:

- +7 day grace period
- Domain deleted permanently after a 90 day quarantine period

Important:

- Existing domains being updated, transferred, or assigned to a new owner can only receive a maximum classification of “Suspicious”
- Domain remains active during verification

High Risk

- Domain immediately **on hold**
- New domains stay in **pending create** and not activated righ away.

Typical reason: highly suspicious or false holder data.

---

3. Verification Timeline

For Suspicious Cases

Stage	Timeline	Result
Verification requested	Day 0	Reseller receives email from Openprovider
Initial deadline	Within 30 days	Verification must be completed
Grace period	Additional 7 days	Final chance to verify
Quarantine	Up to 90 days	Domain stops resolving
Final deletion	After quarantine	Domain is permanently deleted

Notes:

- DNS stays stored during quarantine
- No Redemption Grace Period
- Transfers do NOT reset deadlines
- Previous verification does NOT carry over

---

4. Responsibilities

Openprovider	Reseller
Sends reseller email with: • Domain name • Holder details • Deadline• Instructions	Must: • Contact customer • Confirm holder details • Collect supporting proof • Send confirmation to Openprovider

---

5. Required Documents

Individuals	Organizations
Must verify: • Person exists • Address belongs to them **Accepted:** • Passport • National ID • Driver’s license • Utility bill • Bank statement **Best practice:** • Govt ID to verify name • Utility bill/bank statement for address	**Must verify:** • Legal existence • Correct address **Accepted:** • Business register extract • Articles of association • Partnership agreement • Founding documents • Utility bill • Bank statement **Best practice:** • Use business registration documents to verify the organization

---

6. DENIC Direct Communications

DENIC contacts the holder directly:

Stage	DENIC Communication

Before Quarantine	**Dedelegation Warning**→ Risk of domain going offline
During Quarantine	**Dedelegation Information**→ Domain is offline
Before Deletion	**Notice of Termination**→ Domain will be deleted

Important:

- Sent by DENIC (not Openprovider)
- May be sent by post if email fails
- Customers may contact you

---

7. If Verification Fails

- Openprovider informs DENIC
- DENIC grants 7 day final period
- 90-day quarantine
- Domain stops resolving
- Permanent deletion

Impact:

- If multiple domains using same contact → all affected

---

8. Upcoming Automation (KYC/KYB)

Expected: **Coming soon**

New Flow

Step 1 – Reseller Notification

- Informational only
- No immediate action required

Step 2 – Customer Verification

- Email from: `noreply@registrar.eu`
- White-label (includes reseller name)
- Secure upload link

→ Customer uploads documents directly

What Changes for Resellers

You no longer need to:

- Collect documents
- Store documents
- Send proof manually

Step 3 – Pre-Verified Holders

- Openprovider auto-submits data
- Higher chance of **Low Risk**

Step 4 – New Dashboard

RCP → Contact Verifications

You can:

- View open verification requests
- Track status
- Monitor deadlines

9. Recommended Actions

- Inform customers about increased verification
- Keep contact details accurate
- Monitor Openprovider emails
- Train support teams on DENIC notices
- Act quickly on requests

Best practice:

Verified and accurate holder information should result in a low risk classification and avoid any service disruption.

9. Frequently Asked Questions

- ## Will the domain stop working immediately?

Only high risk cases are placed on hold immediately. Suspicious cases continue working during the 30-day verification period.

- ## Can a transfer avoid the verification deadline?

No. Transferring the domain to another registrar does not reset the deadline.

- ## Does previous verification with another registrar count?

No. DENIC requires verification through the current registrar process.

- ## What happens during quarantine?

The domain no longer resolves, but DNS records remain stored.

- ## Is there a redemption period after deletion?

No. Once deleted after quarantine, the domain cannot be recovered through a redemption grace period.

- # Can several domains be affected at once?

Yes. If multiple .DE domains use the same contact details, all of them may be affected together.

Revision #5
Created 2026-08-07 14:00:31 UTC by Sarath
Updated 2026-08-13 10:14:16 UTC by Sarath