team.blue Verification Hub (VHub)

Privacy Policy Clause Template

Verification of domain name registrant data

We verify domain name registrant data in connection with domain name registrations, transfers, changes of holder, and contact detail updates, as required by applicable legal, registry or accreditation requirements. Our statutory verification obligations arise under the applicable national provision]implementing Article 28 of Directive (EU) 2022/2555 ("NIS2"), in force and applicable to us. The legal basis for processing your personal data is Art. 6(1)(c) GDPR, to the extent that the processing is necessary to comply with a legal obligation applicable to us.

Personal data processed. We process the registrant's name, e-mail address, telephone number and postal address, together with the domain name and information about the relevant registration-related operation. Where the registrant is an organisation, we also process the personal data of the individual acting on its behalf.

Depending on the verification checks required (see section: "**Verification process and recipients**"), additional personal data may be processed, including telephone verification- and identify-verification related information, as well as technical device data such as IP address, browser and operating system, and location information derived from the IP address in relation to identity verification.

No biometric verification, such as selfie matching or liveness detection, is performed as part of this process.

Verification process and recipients. The verification is carried out through the central team.blue Verification Hub ("VHub"), operated on our behalf by team.blue NV (Skaldenstraat 121, 9042 Ghent, Belgium), acting as our processor.

Depending on the applicable registry, accreditation and legal requirements, and the outcome of an automated risk assessment based on the domain name, VHub determines which verification checks are required. Email verification, a default process, is performed directly by VHub by sending the registrant a verification link and code.

Where legally required, telephone verification is performed by DING NEGOCE SAS (82 rue Dutot, 75015 Paris, France), through the Prelude service, acting as a sub-processor of team.blue NV. DING will receive your telephone number, the selected delivery method and the language used for verification. The privacy policy of DING is available at the following link: DING Privacy Policy.

Where legally required, including where the risk assessment indicates medium or high risk or where the relevant registry requires it, identity verification is performed by ComplyCube (Teemo Technology Ltd, London), acting as a sub-processor of team.blue NV. ComplyCube verifies the authenticity of the identity document and extracts information from it using automated data extraction. ComplyCube also processes technical device data, such as IP address, browser and operating system, and location information derived from the IP address. VHub does not receive or store the identity document itself. The privacy policy of ComplyCube is available at the following link: ComplyCube Privacy Policy.

Automated verification process. The verification process uses automated checks. The checks performed depend on applicable requirements and the outcome of the risk assessment. If the required verification is unsuccessful, we will not be able to carry out the requested operation. For an existing domain name, failure to complete the required verification may result in further measures, including suspension or deletion of the domain name registration, in accordance with applicable legal and registry requirements and our published policies.

Verification results and disclosures. VHub records the verification method, outcome and relevant timestamps and communicates the overall verification status and attempt identifier to our business system. We may share the verification status with registries where required by applicable requirements. We may also disclose verification evidence to registries or competent authorities, where legally required, including in response to a lawful request.

Data retention. We retain verification records for as long as necessary to comply with applicable legal, registry and accreditation requirements, and, where necessary, to establish or defend legal claims. Verification records and evidence retained by our service providers are subject to the relevant contractual arrangements and applicable legal and regulatory requirements.