

RDDS Richtlinie für .versicherung Domains

1. Definitionen:

- RDDS** RDDS (Registration Data Directory Services) bezeichnet die Gesamtheit der Dienste, die von Registries und Registraren angeboten werden, um Zugriff auf Domain-Registrierungsdaten zu gewähren, z.B. mittels RDAP, früher auch Whois.
- RDAP** Das Registration Data Access Protocol (RDAP) ermöglicht Benutzern den Zugriff auf aktuelle Registrierungsdaten.

2. Richtlinie

1. tldbox GmbH (nachstehend als „Registry“ bezeichnet) stellt der Öffentlichkeit für .versicherung-Domains für RDDS-Abfragen einen RDAP-Server zur Verfügung, auf den unter „rdap.nic.versicherung“ zugegriffen werden kann.
2. Die Registry kann zeitweilig nach freiem Ermessen bestimmte Grenzen bezüglich der Anzahl gleichzeitiger und/oder aufeinander folgender Anfragen festlegen.
3. Seit dem Inkrafttreten der DSGVO (Datenschutz-Grundverordnung, <https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679>), der NIS2-Richtlinie (in der Umsetzung österreichisches NISG 2026, <https://ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20013065>) sowie der entsprechenden Richtlinien von ICANN sind die Daten des Registranten, sofern dieser eine natürliche Person ist, sowie etwaiger weiterer Kontakte grundsätzlich nicht mehr öffentlich zugänglich.

3. Regeln

1. Der Registrar muss sicherstellen, dass die tatsächlichen Angaben in den Datenfeldern zum Registrant, wie von der Registry definiert, vom Registrant selbst stammen, und der Registrar muss diese Daten erfassen und laufend aktualisieren.
2. Der Registrar muss den Registrant darüber informieren, dass der Datensatz, falls veröffentlicht, selbst nach der Entfernung einer Domain aus der Root-Zone noch 24 Stunden lang am RDAP-Server angezeigt werden kann.
3. Die Registry kann die Korrektheit und Vollständigkeit der Registrant-Daten jederzeit anhand zufällig ausgewählter Domains prüfen. Wenn Fehler vorliegen oder Daten fehlen, wird der zuständige Registrar darüber informiert, der diese Mängel innerhalb von 21 Tagen mit den betreffenden Registranten beheben muss.
4. Die Registry erfüllt alle von ICANN in den Consensus- oder temporären Richtlinien (gemäß Definition im Registry-Vertrag) geforderten Sicherheits-, RDDS- und Datenschutzvorgaben. Außerdem erfüllt die Registry sämtliche nationalen gesetzlichen Vorschriften sowie behördlichen Auflagen.
5. Registranten senden Anfragen bezüglich Änderungen, Aktualisierungen und/oder Korrekturen ihrer-Daten an den für sie zuständigen Registrar. Der Registrar prüft und authentifiziert diese Anfragen und nimmt nach einer erfolgreichen Prüfung und Authentifizierung der Anfrage innerhalb von 10 Tagen die notwendigen Änderungen vor.

6. Mit der Einreichung einer RDAP-Anfrage willigt der Anfragende ein, die dadurch erhaltenen Informationen ausschließlich für rechtmäßige Zwecke zu verwenden und weder jetzt noch in Zukunft
 - a. die Übermittlung unverlangter Massenwerbung per Post, E-Mail oder Telefon zu erlauben, zu ermöglichen, zu vermitteln und/oder zu fördern;
 - b. gegen geltende Datenschutzgesetze und Gesetze zum Schutz der Privatsphäre zu verstoßen und
 - c. großvolumige automatisierte und/oder elektronische Prozesse zur Abfrage der Datenbank zu nutzen und/oder zu ermöglichen.
7. Alle über eine RDAP-Abfrage erhaltenen Daten werden „in der vorliegenden Form“ und ohne Zusage und/oder Gewährleistung bezüglich ihrer Genauigkeit bereitgestellt. Die Registry übernimmt unter keinen Umständen Verantwortung und/oder Haftung für die Zuverlässigkeit von über eine RDAP-Abfrage erhaltenen Daten.
8. Die Offenlegung von Kontaktdaten ist durch geltendes Datenschutzrecht eingeschränkt. Die Kontaktdaten für bestimmte Domains sind daher möglicherweise nur eingeschränkt zugänglich.
9. Alle Urheberrechte an RDDS-Informationen, der RDDS-Datenbank und den Datensätzen sind ausdrücklich der Registry vorbehalten.
10. Es ist streng untersagt, über RDDS-Services erhaltene Informationen zu kombinieren, zu sammeln und/oder zu kompilieren.