

Zertifikate, Versicherungen & TOM

Stand: 04/2026

dataroom^x
Der sichere deutsche Datenraum

IONOS



Deutschlands sicherer und einfacher Datenraum



dataroomX[®] unterstützt

- als eines von vierzehn Mitgliedern des Kompetenznetzwerk Trusted Cloud e. V. – Herausgeber des Gütesiegels für vertrauenswürdige Cloud Services, initiiert vom Bundesministerium für Wirtschaft, und



- als Teilnehmer die deutsche Allianz für Cyber-Sicherheit – eine Initiative des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Erhöhung der Cyber-Sicherheit in Deutschland.



Höchste Datenschutz- und Sicherheitsanforderungen nach der Schutzanforderungsklasse 3 und Datenschutzgrundverordnung

dataroomX[®] gewährleistet durch risikoangemessene technische und organisatorische Maßnahmen nach dem Stand der Technik, dass die Daten nicht unbefugt verarbeitet oder genutzt werden können. Die Maßnahmen sind nach dem Stand der Technik geeignet, um solche Vorgänge aufgrund technischer oder organisatorischer Fehler einschließlich Bedienfehlern, oder fahrlässiger oder vorsätzlicher Handlungen durch den Cloud-Anbieter und seine Mitarbeiter oder Dritte (andere Cloud-Nutzer, sonstige Dritte) hinreichend sicher auszuschließen. Dazu gehören insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Verfahren zur Erkennung von Missbräuchen.



Zertifikat

für das Managementsystem nach
ISO/IEC 27001 : 2022

Die Zertifizierungsstelle TÜV NORD CERT GmbH bestätigt hiermit als Ergebnis der Auditierung, Bewertung und Zertifizierungsentscheidung gemäß ISO/IEC 27006:2015/Amd.1:2020, dass die Organisation

IONOS Holding SE
Elgendorfer Straße 57
56410 Montabaur
Deutschland

ein Managementsystem konform zu den Anforderungen der ISO/IEC 27001 : 2022 am Standort

IONOS SE
Elgendorfer Straße 57
56410 Montabaur
Deutschland

betreibt und innerhalb der Laufzeit des Zertifikats von 3 Jahren auf Konformität überwacht wird.

Geltungsbereich

Betrieb und Entwicklung von Infrastruktur, Plattformen und Applikationen für Internetprodukte und -dienstleistungen in den Rechenzentren der IONOS sowie der zugehörige Kundenservice

Unter Berücksichtigung der Erklärung zur Anwendbarkeit vom 03.03.2025 (Version 5.0)

Zertifikat-Registrier-Nr. 44 121 180247-012 Gültig von 2025-04-19
Auditbericht-Nr. 9559 4141 Gültig bis 2028-04-18
Erstzertifizierung 2021

Essen, 2025-04-18 

Zertifizierungsstelle der TÜV NORD CERT GmbH

Dieses Zertifikat ist gültig in Verbindung mit dem Hauptzertifikat.

TÜV NORD CERT GmbH
Am TÜV 1, 45307 Essen
www.tuev-nord-cert.de

TÜV®







Nutzen Sie unsere Datenbank, um die Zertifikatsgültigkeit zu verifizieren.

Die Norm ISO/IEC 27001 spezifiziert Vorgaben für den Aufbau eines Informationssicherheits-Managementsystems (ISMS). Der international gültige Standard bildet die Basis für Betrieb und Entwicklung aller Produkte und Prozesse in der gesamten IONOS Gruppe, einschließlich aller Ressourcen von Drittanbietern.

DCNW ISO/IEC 27001:2022 Zertifikat

Server www.dataroomx.de

Geografischer Standort des Rechenzentrums: Deutschland

Geografischer Standort des Backup-Rechenzentrums: Deutschland

– Gültig bis 2028 –



Testat des Bundesamtes für Sicherheit in der Informationstechnik zum Betrieb der Produkte Compute Engine, S3 Object Storage, Managed Backup und Managed Kubernetes in Deutschland

BSI Testat IT-Grundschutz

Server www.dataroomx.de

Geografischer Standort des Rechenzentrums: Deutschland

Geografischer Standort des Backup-Rechenzentrums: Deutschland

– Gültig bis 2028 –

Ionos Cloud

1&I Ionos SE

< Zurück zur Übersicht

Servicebeschreibung

Die Ionos Cloud ist eine öffentliche (public) IaaS-Lösung, zugeschnitten auf die Bedürfnisse von KMU, Entwicklern und Value Added Resellers, vereint die Ionos Cloud alle Vorteile eines physischen Servers mit den erweiterten Möglichkeiten der Cloud.

Zum Angebot

Ergebnis Teilen

Trusted Cloud Label für vertrauenswürdige Cloud Services für die
Wirtschaft

Zertifikatsnr.: 2261

<https://www.trusted-cloud.de/cloudservices/2261/Ionos-Cloud.html>

Das Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) ist der im Technologieprogramm Trusted Cloud des Bundesministeriums für Wirtschaft und Energie (BMWi) entwickelte Prüfstandard für die Datenschutz-Zertifizierung nach dem Bundesdatenschutzgesetz (BDSG).

– Gültig –

Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO als Anlage zu einem/mehreren vom Auftraggeber genutzten Vertrag/Verträgen

Zwischen der Firma

1&1 IONOS SE
Elgendorfer Straße 57
56410 Montabaur
Deutschland

– Nachfolgend „**Auftragnehmer**“ genannt –

und

Firma: **rdts Internet AG, dataroomX**
Name: **Thomas Stiren**
Straße, Hausnummer: **Am Wissenschaftspark 7**
Postleitzahl, Ort: **54296 Trier**
Land: **Deutschland**
Kundennummer: **422190141**

– Nachfolgend „**Auftraggeber**“ genannt –

Vertrag zur Auftragsverarbeitung (AVV)

Einen Vertrag zur Auftragsverarbeitung (AVV) muss nach EU-Datenschutz-Grundverordnung (DSGVO) jede verantwortliche Stelle abschließen, die personenbezogene Daten im Auftrag verarbeiten lässt.

– Explizite Bestätigung der rechtskonformen Umsetzung der gesetzlichen Vorgaben zum Datenschutz durch die 1&1 IONOS SE für rdts Internet AG –

SSL Zertifikat ist richtig installiert

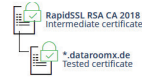
10.02.2021

Informationen über das Zertifikat:

DV Dieser Server nutzt ein domänvalidiertes (DV) Zertifikat. Informationen über den Seitenbetreiber konnten nicht bestätigt werden. Die Daten sind zwar geschützt, doch es wird nicht empfohlen vertrauliche Personen- und Finanzdaten auszutauschen.

Common name: *.dataroomx.de
 SAN: *.dataroomx.de, dataroomx.de
 Organisation:
 Organization unit:
 Stadt/Ort: Bundesland/Gebiet: Land: Certificate Transparency: Embedded in certificate
 Gültig seit: NaN-NaN-NaN NaN-NaN-NaN
 Gültig bis: NaN-NaN-NaN NaN-NaN-NaN
 Seriennummer: 02052041c18f23fd880b5df61177629
 Algorithmus: SHA256withRSA
 Verschlüsselungsstärke: 2048
 Status des Zertifikats: Valid
 Revocation check method: OCSP

Zertifikatskette



RapidSSL RSA CA 2018 (Intermediate certificate)

Common name: RapidSSL RSA CA 2018
 Gültig seit: NaN-NaN-NaN NaN-NaN-NaN
 Gültig bis: NaN-NaN-NaN NaN-NaN-NaN
 Status des Zertifikats: Valid
 Revocation check method: OCSP
 Organisation: DigiCert Inc
 Organization unit: www.digicert.com
 Stadt/Ort:
 Bundesland/Gebiet:
 Land: US
 Certificate Transparency: Not embedded in certificate
 Seriennummer: 08a5246c4db5c8c3d702b4bbab5349
 Algorithmus: SHA256withRSA
 Verschlüsselungsstärke: 2048

***.dataroomx.de (Tested certificate)**

Common name: *.dataroomx.de
 SAN: *.dataroomx.de, dataroomx.de
 Gültig seit: NaN-NaN-NaN NaN-NaN-NaN
 Gültig bis: NaN-NaN-NaN NaN-NaN-NaN
 Status des Zertifikats: Valid
 Revocation check method: OCSP
 Organisation:
 Organization unit:
 Stadt/Ort:
 Bundesland/Gebiet:
 Land:
 Certificate Transparency: Embedded in certificate
 Seriennummer: 02052041c18f23fd880b5df61177629
 Algorithmus: SHA256withRSA
 Verschlüsselungsstärke: 2048

Serverkonfiguration

Host Name php1s.rdt.s.de
 Servertyp Apache
 IP Adresse 82.223.13.174
 Portnummer 443
 Session resumption (caching): Enabled
 Next Protocol Negotiation: Not Enabled
 Downgrade attack prevention: Enabled
 Session resumption (tickets): Enabled
 Secure Renegotiation: Enabled
 Strict Transport Security (HSTS): Not Enabled
 SSL/TLS compression: Not Enabled
 Heartbeat (extension): Enabled
 RC4: Not Enabled
 OCSP stapling: Not Enabled

Geprüftes Schadenpotenzial:

Heartbleed
 Poodle (TLS)
 Poodle (SSLv3)
 FREAK
 BEAST
 CRIME

Aktive Protokolle

TLS 1.2
 TLS 1.1
 TLS 1.0

Inaktive Protokolle

SSLv2
 SSLv3

Verfügbare Cipher Suites:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006B)
 TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)
 TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009A)
 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009F)
 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009E)
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F)
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC030)

Zertifizierung der Datenräume mit einem verschlüsselten Netzwerkprotokoll zur hochsicheren Übertragung von Daten
 Zertifizierung „SSL“

Name: *.dataroomx.de

Web Applications

Zertifikat-Registrier-Nr. : 1F:82:D1:03:A4:BD:

RapidSSL RSA CA 2018

Google Public DNS

RR type: SOA Disable DNSSEC validation Show DNSSEC detail

Result for **www.dataroomx.de/SOA** with DNSSEC validation and without DNSSEC detail:

```
{
  "Status": 0 /* NOERROR */,
  "TC": false,
  "RD": true,
  "RA": true,
  "AD": false,
  "CD": false,
  "Question": [
    {
      "name": "www.dataroomx.de.",
      "type": 6 /* SOA */
    }
  ],
  "Authority": [
    {
      "name": "www.dataroomx.de.",
      "type": 6 /* SOA */,
      "TTL": 1800,
      "data": "ns1.epag.net. postmaster@epag.net. 20200826186400 1800 60 866 86400"
    }
  ],
  "Comment": "Response from 216.129.52.75."
}
```

You may also resolve directly at: <https://dns.google/resolve?name=www.dataroomx.de&type=SOA>

SOA CAT OS18A Classe V 2022

Domain: www.dataroomx.de

– Gültig –

1	2	3	4	5	6	7
1	a) Firma b) Sitz, Niederlassung, Inländische Geschäftsanschrift, empfangsberechtigte Person, Zweigniederlassungen c) Gegenstand des Unternehmens	50.000,00 EUR	a) Allgemeine Vertretungsregelung b) Vorstand, Leitungsorgan, geschäftsführende Direktoren, persönlich haftende Gesellschafter, Geschäftsführer, Vertretungsberechtigte und besondere Vertretungsbefugnis	Prokura	a) Rechtsform, Beginn, Satzung oder Gesellschaftsvertrag b) Sonstige Rechtsverhältnisse	a) Tag der Eintragung b) Bemerkungen
	rdts Internet Aktiengesellschaft Trier Gegenstand des Unternehmens ist die Erstellung und Entwicklung von eigenen und fremden Programmen zur Datenverarbeitung und -bearbeitung, deren Vervielfältigung, Lizenzierung und weiterer Vertrieb sowie Schaltung der Anwerder. Desweiteren Dienstleistungen im Bereich der Einführung und des Betriebs von Informationstechnologien sowie der Vertrieb und der Handel mit Software und Anlagen der Informationstechnologie. Die Gesellschaft betreibt Forschung, Entwicklung, Beratung und Durchführung von Testverfahren im Bereich neue Kommunikations- und Informationstechnologien sowie die wirtschaftliche Verwertung dieser Leistungen sowie Vertriebs entsprechender Produkte. Schließlich betätigt sie sich auf dem Feld der Konzeption, Produktion und Vermarktung von Unternehmens- und Produktpräsentationen in der Internet- Publikationsplattform World Wide Web und auf CD-ROM sowie im Bereich der Implementierung von Produkt- und Bestellatendatenbanken im elektronischen Geschäftsverkehr.		Die Gesellschaft wird durch zwei Vorstandsmitglieder oder durch ein Vorstandsmitglied gemeinsam mit einem Prokuristen vertreten. b) Vorstand: Detemple, Raphael M., Trier, *06.07.1972 Einzervertretungsberechtigt mit der Befugnis im Namen der Gesellschaft mit sich im eigenen Namen oder als Vertreter eines Dritten Rechtsgeschäfte abzuschließen Vorstand: Stiren, Thomas, Trier, *23.11.1970 Einzervertretungsberechtigt mit der Befugnis im Namen der Gesellschaft mit sich im eigenen Namen oder als Vertreter eines Dritten Rechtsgeschäfte abzuschließen		a) Aktiengesellschaft Satzung vom 24.06.1999	a) 01.12.2005 Lange b) Tag der ersten Eintragung: 06.09.1999 Dieses Blatt ist zur Fortführung auf EDV umgeschrieben worden und an die Stelle des bisherigen Registrierblattes des Amtsgerichts Trier getreten. Freigegeben am 01.12.2005. Satzung Blatt 14 ff. Sonderband
2	b) Gemäß § 18 FGAHRG von Amts wegen erhöhtlagen: Geschäftsanschrift: Herzogenbuscher Straße 14, 54292 Trier					a) 21.04.2010 Sökenberger
3	b) Änderung der Geschäftsanschrift: Am Wissenschaftspark 7, 54296 Trier					a) 06.06.2011 Assmann

Hiermit erkläre ich, dass unsere Aktiengesellschaft wie folgt
gehalten wird:

50 % Raphael M. Detemple

50 % Thomas Stiren

Wir sind deutsche Staatsbürger.



Thomas Stiren

Vorstand rdts Internet AG

Trier, 27. Oktober 2025

Dokumentation des Verfahrens

Nach Projektabschluss erfolgt die revisionssichere Versiegelung der Daten durch einen Notar.

Diese Daten werden direkt an den vereidigten Notar zur Versiegelung des Datenraums per gesicherter Mail mit passwortgeschütztem Systemdownload gesendet.

Die DVDs werden vom Notar beschrieben, schreibgeschützt versiegelt und können nicht mehr bearbeitet werden. Der Notar beglaubigt diesen Vorgang zusätzlich schriftlich.

Das Revisionsprotokoll hält fest:

- Welche Nutzer haben wann welche Daten heruntergeladen?
- Welche Administratoren haben wann welche Daten hochgeladen, verändert oder gelöscht?

Wir gewährleisten durch die Übertragung auf eine notarielle Hoheitsaufgabe u. a. die

- Ordnungsmäßigkeit der Übergabe und den
- Schutz vor Veränderungen und Fälschungen.

Außerdem bestätigen wir die

- Vollständigkeit der archivierten Unterlagen (Nutzung nur durch Berechtigte mit eventuellen Einschränkungen in der Administration)
- Sicherheit der Bearbeitung, Archivierung und Aufbewahrung
- Sicherung vor Verlust durch Backups, ausgelagerte Daten u.ä.



Notar Dr. Thorsten Hilger
Mühlenberg 12
54662 Speicher

Mit der Schließung des Datenraumes werden alle Daten binnen 90 Tagen von allen Servern (Echtserver, Notfallserver, externe Backups) gelöscht. Eine Archivierung oder Aufbewahrung erfolgt nach diesem Zeitraum nicht mehr.

Berufshaftpflichtversicherung (bis 2 Mio. €):

Name: Hiscox Europe Underwriting Limited

Anschrift: Arnulfstraße 31, 80636 München

Räumlicher Geltungsbereich: Bundesrepublik Deutschland

Betriebshaftpflichtversicherung (bis 3 Mio. €):

Name: Württembergische Versicherung AG

Anschrift: Gutenbergstraße 30, 70176 Stuttgart

Räumlicher Geltungsbereich: Bundesrepublik Deutschland

Allgemeine Geschäftsbedingungen (AGB)

Stand: 1. August 2017

<https://www.dataroomx.de/datenraum-agb>

Vereinbarung zur Datenverarbeitung im Auftrag

Stand: 17. Februar 2025

<https://www.dataroomx.de/auftragsdatenverarbeitung>

Datenschutzerklärung

Stand: 25. Januar 2019

<https://www.dataroomx.de/datenraum-datenschutz>

Technische und organisatorische Maßnahmen/Zweck, Art und Umfang der Auftragserarbeitung, Art der Daten und Kategorien betroffener Personen

https://www.dataroomx.de/auftragsdatenverarbeitung/#_anlage1

Datenschutzbeauftragter

Felicia Steiner, datenschutz@dataroomx.de

Datenschutz-Folgenabschätzung (DSFA) für dataroomX[®]

Einleitung:

Dieses Dokument soll die potenziellen Datenschutzrisiken untersuchen, die mit der Nutzung von dataroomX[®], verbunden sind. Die DSFA dient dazu, die Einhaltung der Datenschutz-Grundverordnung (DSGVO) zu gewährleisten und Risiken für die Rechte und Freiheiten natürlicher Personen, die aus der Datenverarbeitung resultieren könnten, zu minimieren.

1. Beschreibung des Verarbeitungsvorgangs:

dataroomX[®] ist ein digitaler Datenraum, in den Nutzer unterschiedlichste Dokumente hochladen können. Obwohl wir als Datenraum-Provider nicht wissen, welche spezifischen Dokumente abgespeichert werden, haben wir technische und organisatorische Maßnahmen getroffen, um die Datenintegrität und -sicherheit zu gewährleisten.

2. Zweck und Rechtsgrundlage der Verarbeitung:

Der Hauptzweck von dataroomX[®] ist es, einen sicheren und effizienten Raum für Due-Diligence-Prozesse bereitzustellen. Die Rechtsgrundlage für die Datenverarbeitung kann, je nach Kontext, auf Vertragserfüllung, berechtigtem Interesse oder expliziter Einwilligung des Nutzers basieren.

3. Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung:

Die Verarbeitung ist notwendig, um den Nutzern eine sichere Plattform zur Speicherung und zum Austausch von Dokumenten zu bieten. Datensicherheitsmaßnahmen sind proportional und entsprechend dem Risiko ausgerichtet.

4. Risikobewertung:

Obwohl dataroomX® hohe Sicherheitsstandards einhält, bestehen immer Risiken. Dazu gehören potenzielle Datenlecks, unberechtigter Zugriff oder Datenverlust. Diese Risiken sind jedoch durch strenge Sicherheitsprotokolle und regelmäßige Überprüfungen minimiert.

5. Maßnahmen zur Risikominderung:

Wir haben eine Reihe von Sicherheitsmaßnahmen implementiert, die sich aus Zertifizierungen, Verschlüsselungstechnologien, regelmäßige Backups, Sicherheitsschulungen und kontinuierliche Sicherheitsüberwachung und -updates ergeben und über die ADD/TOM erfasst sind.

Die Nutzung von dataroomX® ist, unter Berücksichtigung der implementierten Sicherheitsmaßnahmen, aus datenschutzrechtlicher Sicht sicher. Dennoch sollten Nutzer stets wachsam bleiben und sicherstellen, dass sie nur die notwendigen Daten hochladen und teilen.

Auszug aus dem Maßnahmenkatalog zum Notfallmanagement nach BSI-Vorgaben

Unser Notfallmanagement wurde durch die IT-Grundschutzkataloge des BSI für detaillierte Informationen zur Gestaltung von Informationssicherheit und Notfallmanagements erstellt. Wir haben uns über Dienstleistungen qualifizierter IT-Sicherheitsdienstleister auf den Webseiten des BSI informiert.

Ansprechpartner für IT-Notfälle:

Beauftragter Informationssicherheit: F*****

Beauftragter Notfallmanagements: T*****

Präambel:

1. Kritische Prozesse werden halbjährlich nach Business Impact Analyse identifiziert.
2. Für die interne und externe Kommunikation sind Kommunikationswege festgelegt, um potenziellen Imageschaden zu begrenzen.
3. Wir installieren Sicherheitsupdates, setzen Schutzprogramme ein, nutzen Firewalls, ändern Standardpasswörter und erstellen regelmäßige Backups. Wir überprüfen regelmäßig den Sicherheitsstatus unserer IT-Systeme.
4. Die Mitarbeiter kennen die Ansprechpartner für IT-Notfälle.
5. Wir schulen und sensibilisieren unser Personal im Umgang mit IT-Systemen und zum Verhalten im IT-Notfall.

IT-Notfall-Plan:

1. Patient Zero identifizieren: Wir ermitteln den Einstiegspunkt des Cyber-Angriffs, um das Ausmaß der Kompromittierung zu verstehen.
2. Kommunikation koordinieren: Wir kontaktieren sofort alle notwendigen Ansprechpartner in unserem Unternehmen.
3. Informationen sammeln und sichern: Wir sammeln und sichern alle relevanten Informationen (System-Protokolle, Log-Dateien, etc.) für eine eventuelle forensische Auswertung.
4. Meldepflichten beachten: Wir prüfen Meldepflichten und kontaktieren ggf. die Zentrale Ansprechstelle für Cybercrime (ZAC) oder das Bundesamt für Verfassungsschutz.

Nachbereitung

1. Netzwerküberwachung intensivieren: Wir überwachen und monitorieren unser Netzwerk und unsere IT-Systeme nach einem Cyber-Angriff besonders intensiv.
2. Lessons Learned anwenden: Wir prüfen, welche Regelungen, Maßnahmen oder Prozesse optimiert und abgesichert werden müssen.
3. Dokumentation aktualisieren: Wir halten unsere Dokumentation zum Notfallmanagement stets auf dem aktuellen Stand.

Service Level Agreement von dataroomX®

Dieses SLA ist ein wesentlicher Teil des Kundenvertrags und legt die Bedingungen für die von dataroomX® angebotenen Dienste sowie den Mindestumfang der Kundenansprüche fest, ergänzend zu den AGB.

1. Verfügbarkeit

dataroomX® verpflichtet sich, wirtschaftlich vertretbare Anstrengungen zu unternehmen, um eine Verfügbarkeit der Datenräume von mindestens 99,95 Prozent im monatlichen Durchschnitt zu gewährleisten. Bei Nichterfüllung dieser Verpflichtung ist eine Entschädigung ausgeschlossen.

2. Support-Anfragen

Bei Eingang einer Support-Anfrage wird ein qualifizierter Systemadministrator Kontakt mit Ihnen aufnehmen. Die Anfragen werden gemäß den unten aufgeführten Reaktionszeiten bearbeitet.

Tel. +49 651 84031-112
notfall@dataroomx.de

3. Folgende Reaktionszeiten gelten für Support-Anfragen

- Bei einer Störung (Service nicht verfügbar oder eingeschränkt nutzbar): < 1 Stunde
- Bei Service- oder Informationsanfragen: < 6 Stunden

Innerhalb der festgelegten Zeiten antwortet ein Fachexperte mit einer Abschlusserklärung oder einer ersten Einschätzung und weiteren Schritten. Bei Störungen informiert er auch über Ausmaß und voraussichtliche Behebungsdauer.

4. Wartungsarbeiten

dataroomX® kann den Servicezugang vorübergehend beschränken oder aussetzen, um Netzwerksicherheit, -integrität, Serviceinteroperabilität und Datenschutz zu gewährleisten, vorzugsweise während nutzungschwacher Zeiten. Quartalsweise dürfen Wartungsarbeiten den Service nicht länger als vier Stunden unterbrechen. Kunden werden mindestens zwei Arbeitstage vor geplanten und sieben Tage vor längeren Wartungen informiert, ohne die Störungsbehebung zu verzögern. Diese Beschränkungen gelten nicht als Serviceausfallzeiten.

5. Haftungsausschluss

Ereignisse, die unvorhersehbar, unvermeidbar und außerhalb des Einflussbereichs von dataroomX® liegen sowie nicht zu vertreten sind, wie höhere Gewalt, Krieg, Naturkatastrophen oder Arbeitskämpfe, entbinden dataroomX® für deren Dauer von der Leistungspflicht. Detaillierte Informationen finden Sie in den AGB.

Registriert im Transparenzregister der Bundesrepublik Deutschland

Registrierungsnummer der transparenzpflichtigen Rechtseinheit:

6400089092


rdts Internet Aktiengesellschaft



Zweck des Transparenzregisters ist die Verhinderung von Geldwäsche und Terrorismusfinanzierung.

Die gesetzlichen Grundlagen finden sich in den §§ 18 ff. Geldwäschegesetz (GwG), der Transparenzregistereinsichtnahmeverordnung (TrEinV), der Transparenzregistergebührenverordnung, der Transparenzregisterbeleihungsverordnung (TBeIV), der Transparenzregisterdatenübermittlungsverordnung (TrDüV) sowie der Indexdatenübermittlungsverordnung (IDÜV).

www.transparenzregister.de



Deutschlands sicherer und einfacher Datenraum

dataroomX®

rdts® Internet AG

Am Wissenschaftspark 7 · 54296 Trier

Postfach 1304 · 54203 Trier

Telefon: 06 51 / 8 40 31-100 · Fax: 06 51 / 8 40 31-122

E-Mail: info@dataroomx.de · Internet: www.dataroomx.de