



Richtlinie zur koordinierten Offenlegung von Schwachstellen

Richtlinie zur koordinierten Offenlegung von Schwachstellen



Inhalt

1.	Dokumenteninformationen	3
	Bearbeitungsvermerk	3
	Änderungshistorie	3
1.1	Gleichstellungshinweis	3
2.	Zweck, Anwendungsbereich und Adressaten	3
3.	Geltungsbereich	3
4.	Meldeweg	4
4.1	Inhalt einer Meldung	4
5.	Unser Umgang mit Ihrer Meldung	4
6.	Zusicherung der DARZ GmbH	4
7.	Regeln für die Untersuchung	5
7.1	Was wir erwarten	5
7.2	Was nicht zulässig ist	5
8.	Koordinierte Offenlegung	5
9.	Vergütung	5
10.	Datenschutz	5
11.	Gesetzliche Meldepflichten	6
12.	Geltung und Überprüfung	6
13.	Sonstiges	6
1.	Purpose, scope and addressees	7
2.	Scope	7
3.	How to report	7
3.1	What a report should contain	7
4.	How we handle your report	8
5.	Our assurance to you	8
6.	Rules of engagement	8
6.1	What we expect	8
6.2	What is not permitted	8
7.	Coordinated disclosure	9
8.	Rewards	9
9.	Data protection	9
10.	Statutory reporting obligations	9
11.	Validity and review	9
12.	Miscellaneous	9

Richtlinie zur koordinierten Offenlegung von Schwachstellen



1. Dokumenteninformationen

Bearbeitungsvermerk

	Name und Funktion	Version	Datum	Unterschrift
Erstellt von:	Tiziana Knecht, ISMS-Beauftragte	1.0	04.09.2026	
Geprüft von:	Raphael Munasypow, Geschäftsleitung	1.0	04.09.2026	
Genehmigt von:	Jürgen Henzler, Geschäftsführer & CISO	1.0	04.09.2026	
Rücknahme durch:				

Änderungshistorie

Datum	Bearbeiter	Version	Änderungsgrund / Änderungen
04.09.2026	Tiziana Knecht Jürgen Henzler	1.0	Erstellung; Veröffentlichung der Meldestelle

1.1 Gleichstellungshinweis

In folgendem Dokument wird für die Beschreibung von Aufgaben, Funktionen oder Rollen aus Vereinfachungsgründen die männliche Schreibweise gewählt. Mit der gewählten Schreibweise werden in diesem Dokument alle Geschlechter angesprochen, denen Aufgaben, Funktionen oder Rollen zugeordnet werden, ohne eine Wertung ihres Geschlechts, ihrer physischen oder psychischen Fähigkeiten, oder eine sonstige Wertung vorzunehmen.

2. Zweck, Anwendungsbereich und Adressaten

Die Sicherheit unserer Systeme und der Daten unserer Kunden hat für die DARZ GmbH hohe Bedeutung. Trotz aller Sorgfalt lassen sich Schwachstellen nie vollständig ausschließen. Diese Richtlinie beschreibt, wie Sie eine Schwachstelle an uns melden können, wie wir damit umgehen und welche Zusicherungen wir Ihnen dabei geben.

Sie richtet sich an alle Personen, die eine Schwachstelle in Systemen, Diensten oder Produkten der DARZ GmbH feststellen, insbesondere an Sicherheitsforscher, Kunden, Partner und Lieferanten. Eine vorherige Anmeldung oder Registrierung ist nicht erforderlich.

Diese Richtlinie ist ein öffentliches Dokument. Sie wird unter www.da-rz.de veröffentlicht und ist über die Datei security.txt unter <https://www.da-rz.de/.well-known/security.txt> auffindbar.

Adressat der Meldungen ist die DARZ GmbH, Julius-Reiber-Straße 11, 64293 Darmstadt. Sie gilt für den Anwendungsbereich des Informationssicherheitsmanagementsystems (ISMS) der DARZ GmbH, der DC Darmstadt GmbH und der WeDoIT S.R.L.

3. Geltungsbereich

In den Geltungsbereich dieser Richtlinie fallen:

- die von der DARZ GmbH betriebenen öffentlich erreichbaren Systeme und Dienste unterhalb der Domäne da-rz.de,
- die von der DARZ GmbH bereitgestellten Kundenportale und Verwaltungsoberflächen,
- Produkte und Softwarekomponenten, die die DARZ GmbH unter eigenem Namen oder eigener Marke bereitstellt.

Nicht in den Geltungsbereich fallen:

- Systeme von Kunden, die im Rechenzentrum der DARZ GmbH untergebracht sind. Für diese ist der jeweilige Kunde verantwortlich. Bitte melden Sie solche Feststellungen dennoch an uns; wir leiten sie an den Verantwortlichen weiter.
- Systeme und Dienste Dritter, die lediglich über Systeme der DARZ GmbH erreichbar sind.
- Feststellungen ohne Sicherheitsrelevanz, etwa fehlende Best-Practice-Header ohne nachweisbare Auswirkung, Ergebnisse automatisierter Scans ohne belegte Ausnutzbarkeit oder Hinweise auf veraltete Versionsstände ohne konkreten Angriffsweg.

Richtlinie zur koordinierten Offenlegung von Schwachstellen



Bestehen Zweifel, ob eine Feststellung in den Geltungsbereich fällt, melden Sie sie bitte. Wir klären die Zuständigkeit und geben Ihnen Rückmeldung.

4. Meldeweg

Melden Sie Schwachstellen ausschließlich an cra@da-rz.de.

Meldeadresse	cra@da-rz.de
security.txt	https://www.da-rz.de/well-known/security.txt
Sprachen	Deutsch, Englisch

Bitte nutzen Sie für Schwachstellenmeldungen nicht die allgemeinen Vertriebs- oder Supportkanäle und veröffentlichen Sie keine Angaben in sozialen Netzwerken, bevor die Meldung bearbeitet wurde.

4.1 Inhalt einer Meldung

Damit wir Ihre Meldung zügig bewerten können, geben Sie bitte an:

- das betroffene System, den betroffenen Dienst oder das betroffene Produkt, möglichst mit URL, IP-Adresse oder Versionsstand,
- eine Beschreibung der Schwachstelle und ihrer möglichen Auswirkung,
- die Schritte zur Nachvollziehbarkeit, gegebenenfalls mit Beleg in Form von Aufzeichnungen oder Bildschirmfotos,
- Datum und Uhrzeit Ihrer Feststellung sowie die verwendeten IP-Adressen, damit wir Ihre Aktivitäten in unseren Protokollen zuordnen können,
- Ihre Kontaktdaten für Rückfragen sowie die Angabe, ob Sie namentlich genannt werden möchten.

Unvollständige Meldungen bearbeiten wir ebenfalls. Fehlende Angaben verzögern jedoch die Bewertung.

5. Unser Umgang mit Ihrer Meldung

Schritt	Frist
Automatische Bestätigung des Eingangs	unverzüglich
Inhaltliche Erstantwort durch einen Ansprechpartner	innerhalb von 2 Arbeitstagen
Rückmeldung zur Bewertung der Meldung	innerhalb von 10 Arbeitstagen
Statusmeldung bei längerer Bearbeitung	mindestens alle 14 Tage

Wir bewerten jede Meldung, halten Sie über den Bearbeitungsstand auf dem Laufenden und informieren Sie, sobald die Schwachstelle behoben ist oder wir entschieden haben, sie nicht zu beheben. Eine ablehnende Entscheidung begründen wir Ihnen gegenüber.

6. Zusicherung der DARZ GmbH

Halten Sie sich an die Regeln nach Abschnitt 6 dieser Richtlinie, so sichert Ihnen die DARZ GmbH zu:

- Wir betrachten Ihre Untersuchung als autorisiert und werden gegen Sie keine zivilrechtlichen Schritte einleiten.
- Wir werden keine Strafanzeige stellen und keinen Strafantrag stellen.
- Sollte ein Dritter wegen Ihrer Untersuchung rechtliche Schritte gegen Sie einleiten, werden wir auf Ihre Anfrage hin bestätigen, dass Ihr Vorgehen dieser Richtlinie entsprach.
- Wir behandeln Ihre Meldung und Ihre Identität vertraulich und geben Ihre Daten nicht ohne Ihre Zustimmung an Dritte weiter, soweit uns nicht gesetzliche Pflichten entgegenstehen.

Richtlinie zur koordinierten Offenlegung von Schwachstellen



Diese Zusicherung kann sich nur auf Ansprüche der DARZ GmbH beziehen. Ansprüche Dritter, insbesondere von Kunden, deren Systeme bei uns untergebracht sind, sowie das Handeln von Strafverfolgungsbehörden von Amts wegen können wir nicht ausschließen. Untersuchen Sie deshalb ausschließlich Systeme, die nach Abschnitt 2 in den Geltungsbereich fallen.

7. Regeln für die Untersuchung

7.1 Was wir erwarten

- Beschränken Sie sich auf das Maß an Zugriff, das zum Nachweis der Schwachstelle erforderlich ist.
- Beenden Sie den Test, sobald Sie Zugriff auf fremde Daten erlangen, und melden Sie den Umstand unverzüglich.
- Löschen Sie sämtliche im Rahmen der Untersuchung erlangten Daten, sobald die Meldung abgeschlossen ist, und bestätigen Sie uns die Löschung.
- Geben Sie uns eine angemessene Frist zur Behebung, bevor Sie Informationen veröffentlichen.
- Handeln Sie so, dass der Betrieb unserer Systeme und die Verfügbarkeit für Kunden nicht beeinträchtigt werden.

7.2 Was nicht zulässig ist

- Angriffe auf die Verfügbarkeit, insbesondere Überlastungsangriffe und Lasttests.
- Social Engineering gegenüber Mitarbeitern, Kunden oder Lieferanten, einschließlich Phishing.
- Der Versuch, physischen Zugang zu Gebäuden oder Rechenzentrumsflächen zu erlangen.
- Das Verändern, Löschen oder Veröffentlichen fremder Daten sowie das Ausleiten von Daten über das zum Nachweis erforderliche Maß hinaus.
- Das Einbringen von Schadsoftware oder das dauerhafte Einrichten von Zugängen.
- Automatisierte Massentests, Brute-Force-Angriffe auf Zugangsdaten und das Versenden von Spam.
- Die Weitergabe der Schwachstelle an Dritte vor Abschluss der Abstimmung nach Abschnitt 7.

8. Koordinierte Offenlegung

Wir befürworten die Veröffentlichung von Schwachstellen, nachdem sie behoben sind, weil dies zur Sicherheit aller beiträgt. Über den Zeitpunkt stimmen wir uns mit Ihnen ab.

Als Richtwert gilt eine Frist von 90 Tagen ab Eingang Ihrer Meldung. Ist die Schwachstelle vorher behoben, kann früher veröffentlicht werden. Erfordert die Behebung mehr Zeit, etwa weil ein Hersteller einbezogen werden muss, schlagen wir Ihnen eine Verlängerung vor und begründen sie.

Betrifft die Schwachstelle ein Produkt eines Dritten, leiten wir die Meldung an dessen Hersteller weiter und stimmen die Offenlegung mit ihm ab. Wir informieren Sie darüber.

Auf Ihren Wunsch nennen wir Sie in der Veröffentlichung namentlich. Ohne ausdrückliche Zustimmung erfolgt keine Nennung.

9. Vergütung

Die DARZ GmbH betreibt kein Bug-Bounty-Programm. Für Meldungen wird keine Vergütung gezahlt. Wir bedanken uns für jede qualifizierte Meldung und nennen Sie auf Wunsch nach Abschnitt 7.

10. Datenschutz

Personenbezogene Daten, die Sie uns im Rahmen einer Meldung übermitteln, verarbeiten wir ausschließlich zur Bearbeitung der Meldung und zur Kommunikation mit Ihnen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO. Nähere Angaben enthält unsere Datenschutzerklärung unter www.da-rz.de.

Sie können eine Meldung auch anonym abgeben. In diesem Fall können wir Ihnen keine Rückmeldung geben und keine Zusicherung nach Abschnitt 5 erteilen.

Richtlinie zur koordinierten Offenlegung von Schwachstellen



11. Gesetzliche Meldepflichten

Die DARZ GmbH kann aufgrund gesetzlicher Vorgaben verpflichtet sein, eine gemeldete Schwachstelle an Behörden zu melden, insbesondere nach Art. 14 der Verordnung (EU) 2024/2847 an das zuständige CSIRT und die ENISA. In diesen Fällen melden wir den Sachverhalt, nicht Ihre Person. Ihre Identität geben wir nur weiter, soweit wir gesetzlich dazu verpflichtet sind.

12. Geltung und Überprüfung

Diese Richtlinie tritt mit ihrer Veröffentlichung in Kraft. Sie wird mindestens jährlich sowie anlassbezogen überprüft und bei Bedarf angepasst. Maßgeblich ist stets die auf www.da-rz.de veröffentlichte Fassung.

13. Sonstiges

Bei mehrsprachigen Versionen des Dokumentes gilt die deutsche Fassung als ausschlaggebend.

Richtlinie zur koordinierten Offenlegung von Schwachstellen



1. Purpose, scope and addressees

The security of our systems and of our customers' data matters to DARZ GmbH. Despite all care, vulnerabilities can never be ruled out entirely. This policy describes how you can report a vulnerability to us, how we handle it, and what assurances we give you in return.

It addresses everyone who identifies a vulnerability in systems, services or products of DARZ GmbH, in particular security researchers, customers, partners and suppliers. No prior registration is required.

This is a public document. It is published at www.da-rz.de and can be found through the security.txt file at <https://www.da-rz.de/.well-known/security.txt>.

Reports are addressed to DARZ GmbH, Julius-Reiber-Strasse 11, 64293 Darmstadt, Germany. The policy applies within the scope of the information security management system (ISMS) of DARZ GmbH, DC Darmstadt GmbH and WeDoIT S.R.L.

2. Scope

The following are within scope:

- publicly reachable systems and services operated by DARZ GmbH under the domain da-rz.de,
- customer portals and administrative interfaces provided by DARZ GmbH,
- products and software components that DARZ GmbH places on the market under its own name or trademark.

The following are out of scope:

- customer systems housed in the DARZ data centre. The respective customer is responsible for these. Please report such findings to us nonetheless; we will forward them to the party responsible.
- third-party systems and services that are merely reachable through DARZ systems.
- findings without security relevance, such as missing best-practice headers without demonstrable impact, automated scan results without proven exploitability, or references to outdated version numbers without a concrete attack path.

If you are unsure whether a finding is in scope, please report it. We will clarify responsibility and come back to you.

3. How to report

Please report vulnerabilities exclusively to cra@da-rz.de.

Reporting address	cra@da-rz.de
security.txt	https://www.da-rz.de/.well-known/security.txt
Languages	German, English

Please do not use our general sales or support channels for vulnerability reports, and do not publish any details on social media before the report has been handled.

3.1 What a report should contain

So that we can assess your report quickly, please include:

- the affected system, service or product, where possible with URL, IP address or version,
- a description of the vulnerability and its potential impact,
- the steps to reproduce it, with recordings or screenshots where helpful,
- the date and time of your finding and the IP addresses you used, so that we can match your activity against our logs,
- your contact details for follow-up questions, and whether you wish to be credited by name.

We also process incomplete reports. Missing details will, however, delay the assessment.

Richtlinie zur koordinierten Offenlegung von Schwachstellen



4. How we handle your report

Step	Target
Automated acknowledgement of receipt	without delay
Substantive first response from a named contact	within 2 working days
Feedback on our assessment of the report	within 10 working days
Status update while the case remains open	at least every 14 days

We assess every report, keep you informed of progress, and tell you once the vulnerability has been fixed or once we have decided not to fix it. We will give you reasons for a decision not to act.

5. Our assurance to you

Provided you follow the rules set out in section 6 of this policy, DARZ GmbH assures you that:

- we consider your research authorised and will not bring civil proceedings against you;
- we will not file a criminal complaint against you;
- should a third party take legal action against you because of your research, we will, on your request, confirm that your conduct was in line with this policy;
- we will treat your report and your identity as confidential and will not pass your data to third parties without your consent, unless we are legally obliged to do so.

This assurance can only cover claims of DARZ GmbH. We cannot exclude claims by third parties, in particular by customers whose systems are housed with us, nor action taken by law enforcement authorities of their own motion. Please therefore confine your research to systems that are in scope under section 2.

6. Rules of engagement

6.1 What we expect

- Limit yourself to the level of access necessary to demonstrate the vulnerability.
- Stop testing as soon as you gain access to third-party data and report that fact immediately.
- Delete all data obtained during your research once the report is closed, and confirm the deletion to us.
- Allow us a reasonable period to remediate before you publish any information.
- Act in a way that does not affect the operation of our systems or their availability to customers.

6.2 What is not permitted

- Attacks on availability, in particular denial-of-service attacks and load testing.
- Social engineering against employees, customers or suppliers, including phishing.
- Attempts to gain physical access to buildings or data centre space.
- Modifying, deleting or publishing third-party data, or extracting data beyond what is needed for proof.
- Introducing malicious code or establishing persistent access.
- Automated mass testing, brute-force attacks against credentials, and sending spam.
- Disclosing the vulnerability to third parties before the coordination under section 7 is complete.

Richtlinie zur koordinierten Offenlegung von Schwachstellen



7. Coordinated disclosure

We support publication of vulnerabilities once they have been fixed, because it improves security for everyone. We agree the timing with you.

As a guideline we work to 90 days from receipt of your report. If the vulnerability is fixed earlier, publication can happen earlier. If remediation needs more time, for instance because a manufacturer has to be involved, we will propose an extension and explain why.

If the vulnerability concerns a third-party product, we forward the report to its manufacturer and coordinate disclosure with them. We will keep you informed.

On request we will credit you by name in the publication. Without your express consent, no attribution takes place.

8. Rewards

DARZ GmbH does not operate a bug bounty programme and does not pay for reports. We are grateful for every qualified report and will credit you on request under section 7.

9. Data protection

We process personal data you send us with a report solely to handle the report and to communicate with you. The legal basis is Art. 6(1)(f) GDPR. Further details are set out in our privacy notice at www.da-rz.de.

You may also report anonymously. In that case we cannot give you feedback and cannot extend the assurance under section 5.

10. Statutory reporting obligations

DARZ GmbH may be legally obliged to report a vulnerability to the authorities, in particular under Art. 14 of Regulation (EU) 2024/2847 to the competent CSIRT and to ENISA. In such cases we report the facts, not your person. We will disclose your identity only where we are legally required to do so.

11. Validity and review

This policy takes effect on publication. It is reviewed at least annually and whenever there is cause, and amended where necessary. The version published at www.da-rz.de is always the authoritative one.

12. Miscellaneous

In the case of multilingual versions of this document, the German version shall prevail.