



Digitaler Datenputz

Corporate Digital Responsibility
Initiative

Checkliste 4: Mehr Datenschutz und -sicherheit

Wichtige Hinweise zur Nutzung:

- Diese Checkliste wurde im Rahmen der Aktion „Digitaler Datenputz 2026“ erstellt und ist eine unverbindliche Orientierungs- und Arbeitshilfe. Sie ersetzt keine individuelle Rechts-, Datenschutz-, IT-Sicherheits- oder sonstige fachliche Beratung und erhebt keinen Anspruch auf Vollständigkeit oder Aktualität.
- Prüfen Sie vor der Anwendung eigenverantwortlich, ob die einzelnen Tipps zu Ihrer Organisation, Ihren Systemen, Prozessen und internen Richtlinien passen. Passen Sie die Inhalte bei Bedarf an und stimmen Sie die Umsetzung mit den zuständigen Stellen ab.
- Bitte beachten Sie insbesondere gesetzliche, behördliche oder vertragliche Aufbewahrungs- und Löschpflichten. Löschen, verändern oder verschieben Sie keine Daten, bevor nicht geprüft wurde, ob Aufbewahrungsfristen, laufende Verfahren, interne Vorgaben oder andere Gründe entgegenstehen. Bei Fragen wenden Sie sich bitte an Ihre Rechtsabteilung, den Datenschutz, die IT-Sicherheit oder weitere zuständige Stellen. Die CDR-Initiative bietet keine Rechtsberatung an.
- Für externe Webseiten und Inhalte Dritter übernimmt die CDR-Initiative keine Verantwortung. Die CDR-Initiative übernimmt außerdem keine Haftung für die genannten Tipps oder Schäden im Zusammenhang mit ihrer Umsetzung, soweit dies gesetzlich zulässig ist. Zwingende gesetzliche Haftungsansprüche bleiben unberührt.

2025 wurden von deutschen Datenschutzbehörden insgesamt 249 Bußgelder für Datenschutzverstöße verhängt und **10.259 Datenpannen** gemeldet (Dunkelziffer unbekannt).¹ Und die Konsequenzen sind teuer: Zum einen verhängen Datenschutzbehörden regelmäßig **Bußgelder in Millionenhöhe**², zum anderen kostet ein Datenleck deutsche Unternehmen im Schnitt 3,87 Millionen Euro pro Vorfall.³

Was viele nicht wissen: Ein erheblicher Teil dieser Risiken entsteht nicht nur durch spektakuläre Hackerangriffe von außen, sondern durch **veraltete, vergessene oder falsch abgelegte Daten** im eigenen Haus sowie den **Fehlversand von Dokumenten**. Alte Kundenlisten, Passwörter in Excel-Tabellen, Scan-Ordner mit Ausweiskopien oder freigegebene Cloud-Links, die längst niemand mehr braucht: All das lauert still in unseren digitalen Ablagen und wird oft jahrelang übersehen.

Digitales Aufräumen ist daher nicht nur eine Frage der Ordnung oder Nachhaltigkeit: Es ist **aktiver Datenschutz**. Wer weniger Daten hält, schützt sich selbst, die Kolleg:innen und die Menschen, deren Daten uns anvertraut wurden. Diese Checkliste hilft dir, die größten Hotspots in deiner Dateiablage zu finden und gezielt zu beseitigen.



Abbildung 1: Design von vectorjuice auf magnific.com

¹ DSGVO-Portal (2026). DSGVO-Bußgelder, Urteile & Sicherheitsvorfälle 2025. Abgerufen von: https://www.dsgvo-portal.de/news/rueckblick_dsgvo-bussgeldverfahren_und_datenpannen_2025.php (15.06.2026)

² Ibid.

³ IBM (2025). Cost of a Data Breach Report 2025. Abgerufen von: <https://www.ibm.com/reports/data-breach> (15.06.2026).

Tipps

Personenbezogene Daten in alten Dateien

- ☐ **Kontaktlisten und Adressdaten prüfen:** Gibt es alte Excel-Dateien, CSVs oder Word-Dokumente mit Namen, Adressen, Telefonnummern oder E-Mail-Adressen von Kund:innen, Bewerber:innen oder Mitarbeitenden? Prüfe, ob diese Kontaktlisten und Adressdaten noch gebraucht werden und lösche sie entsprechend.
- ☐ **Veraltete HR-Unterlagen löschen:** Bewerbungsunterlagen abgelehnter Kandidat:innen dürfen nur begrenzte Zeit aufbewahrt werden (i. d. R. sechs Monate). Gibt es noch ältere Ordner? Wenn ja, lösche diese.
- ☐ **Scan-Ablage prüfen:** Scanner-Outputs landen oft unsortiert auf Laufwerken. Häufig enthalten Scans sensible Inhalte wie bspw. Ausweise, Verträge, Gehaltsabrechnungen. Prüfe die alten Scans und lösche entsprechend.

Zugangsdaten und Passwörter

- ☐ **Passwörter in Textdateien oder Tabellen:** Wurden jemals Zugangsdaten (Passwörter, API-Keys, PINs) in Excel, Word oder Notiz-Dateien gespeichert? Diese sollten gelöscht und in einen Passwort-Manager überführt werden.
- ☐ **Zugangsdaten in E-Mails:** Wurden Passwörter im Klartext per Mail versendet oder empfangen? Diese E-Mails sollten gelöscht werden.
- ☐ **Altes Onboarding-Material:** Enthält altes Onboarding-Material temporäre Erstpasswörter oder Zugangsdaten, die nie aktualisiert wurden? Auch hier lohnt es sich zu Löschen.

Geteilte Laufwerke und falsche Zugriffsrechte

- ☐ **Freigegebene Ordner mit zu weiten Rechten:** Prüfe wer Zugriff auf welche Ordner hat. Ehemalige Mitarbeitende, externe Dienstleister oder Projektpartner:innen sollten möglichst keinen Zugriff auf interne Dateien haben, die nicht aktiv gemeinsam genutzt werden.
- ☐ **Öffentliche Cloud-Links überprüfen:** Wurden Dateien in der Cloud mit „Jeder mit dem Link kann zugreifen“ geteilt? Diese Links sollten geprüft und bei Nichtnutzung deaktiviert werden.
- ☐ **Teamlaufwerke auf veraltete Projekte prüfen:** Alte Projektordner enthalten oft noch sensible Kund:innendaten oder Vertragsunterlagen, die längst hätten archiviert werden sollen. Prüfen und bei Bedarf löschen!

Veraltete Versionen & Duplikate mit sensiblem Inhalt

- ☐ **Dokumentenversionen mit sensiblen Daten:** Frühere Vertragsentwürfe, Kalkulationen oder Angebote enthalten oft detaillierte Preis- oder Kund:innendaten. Lösche ältere Versionen nach Abschluss.
- ☐ **Duplikate auf mehreren Laufwerken:** Wenn dieselben Daten auf drei verschiedenen Laufwerken liegen, vervielfacht sich das Risiko im Fall eines Datenlecks. Prüfe auf solche Duplikate und lösche sie entsprechend.

Papierkorb & temporäre Dateien

- ☐ **Papierkorb ist kein sicheres Archiv:** Gelöschte Dateien im Papierkorb sind noch nicht wirklich weg – und damit weiterhin zugänglich. Der Papierkorb sollte regelmäßig geleert werden.

- ☐ **Download-Ordner prüfen:** Der Download-Ordner ist häufig eine unkontrollierte Ablage für sensible PDFs (Rechnungen, Verträge, Ausweise). Prüfe den Ordner und lösche sensible Dateien entsprechend.
- ☐ **Temporäre Dateien und Cache:** Manche Anwendungen legen temporäre Arbeitsdateien an, die personenbezogene Inhalte enthalten können. Auch diese solltest du prüfen und bei Bedarf löschen.

Aufbewahrungsfristen & Löschpflichten

- ☐ **Gesetzliche Löschpflichten kennen:** Nicht alles darf ewig aufbewahrt werden. Manche Daten müssen gelöscht werden (z. B. nach Vertragsende, nach Bewerbungsprozessen). Eine Abstimmung mit der Rechtsabteilung ist obligatorisch und sollte bedürfnisgerecht umgesetzt werden.
- ☐ **Aufbewahrungsfristen dokumentieren:** Wo es Fristen gibt, sollten diese in der Ordnerstruktur oder durch Metadaten sichtbar gemacht werden. Das hilft beim Einhalten der Fristen.
- ☐ **Archiv vs. Ablage trennen:** Daten, die aus rechtlichen Gründen aufbewahrt werden müssen, sollten in einer klar getrennten, zugangsbeschränkten Archivstruktur liegen und nicht im normalen Teamlaufwerk.

Nutzung und Urheberrecht

Diese Checkliste wurde von der CDR-Initiative im Rahmen der Aktion „Digitaler Datenputz 2026“ veröffentlicht. Die CDR-Initiative freut sich über ihre Nutzung unter Beachtung des Disclaimers auf der ersten Seite.

Die Checkliste ist urheberrechtlich geschützt. Eine unveränderte Vervielfältigung und Weitergabe ist zulässig, sofern die Geschäftsstelle der CDR-Initiative als Herausgeberin und die vollständige Quelle genannt werden:

CDR-Initiative (2026). Digitaler Datenputz 2026 – Checkliste 4: Mehr Datenschutz und -sicherheit. Abrufbar unter: <https://cdr-initiative.de/uploads/files/Digitaler-Datenputz-2026-4-Checkliste-Datenschutz-und-sicherheit.pdf>

Bearbeitungen, Ergänzungen und organisationsspezifische Anpassungen sind kenntlich zu machen und dürfen nicht als unveränderte oder offiziell geprüfte Fassung der CDR-Initiative erscheinen. Für bearbeitete Fassungen empfehlen wir den Zusatz:

Bearbeitet und ergänzt durch: [Name der Organisation], [Jahr].

Die Nutzung des Namens, Logos oder Corporate Designs der CDR-Initiative für bearbeitete oder eigenständig erstellte Fassungen ist nur mit vorheriger Zustimmung der Geschäftsstelle zulässig.

Digitaler Datenputz 2026

Der Digitale Datenputz ist eine gemeinsame Aktion verschiedener Organisationen im Rahmen der CDR-Initiative. Sie unterstützt Mitarbeitende dabei, digitale Daten und Ablagen aufzuräumen, bewusster mit digitalen Ressourcen umzugehen und Datenschutz, Datensicherheit sowie digitale Entlastung im Arbeitsalltag zu stärken.

Die teilnehmenden Organisationen setzen die Aktion eigenständig um und passen die Materialien an ihre eigenen Systeme, Prozesse und Rahmenbedingungen an. Weitere Informationen zur Teilnahme finden Sie [hier](#) und [hier](#).

Über die CDR-Initiative

Ziel der Corporate Digital Responsibility (CDR)-Initiative ist es, digitale Verantwortung zu einer Selbstverständlichkeit für Unternehmen aller Branchen werden zu lassen. Die Initiative will Unternehmen motivieren, die Digitalisierung menschen- und werteorientiert zu gestalten. Mit dem rasanten technologischen Fortschritt rücken der Austausch und das gemeinsame Lernen zunehmend in den Mittelpunkt. Die Initiative wurde im Mai 2018 durch das damalige Bundesministerium der Justiz und für Verbraucherschutz (BMJV) gemeinsam mit Unternehmen ins Leben gerufen. Nach einem zwischenzeitlichen Wechsel der Zuständigkeit in das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) liegt die Verantwortung seit 2025 erneut beim Bundesministerium der Justiz und Verbraucherschutz (BMJV). Seit Januar 2023 wird die Geschäftsstelle der CDR-Initiative durch die Partner ConPolicy – Institut für Verbraucherpolitik und concern betrieben.