kaiserkraft
Mini-Guides

Checkliste – Was gehört wohin?

Ziel:
Auf einen Blick sehen, welche Informationen in Dokumentenschrank, Tresor oder Datensafe gehören, was vernichtet werden muss und wo digitale Sicherung zusätzlich sinnvoll ist.

01 Dokumentenschrank – Für vertrauliche Unterlagen, die regelmäßig benötigt werden.

Typische Inhalte:

- [ ] Personalunterlagen wie Arbeitsverträge, Beurteilungen oder Krankmeldungen – sie müssen sicher, aber schnell erreichbar sein.
- [ ] Finanz- und Buchhaltungsunterlagen wie Rechnungen, Bilanzen oder Steuerunterlagen, die regelmäßig verarbeitet werden.
- [ ] Laufende Verträge mit Kunden, Lieferanten und Partnern – der Zugriff sollte klar geregelt sein.
- [ ] Interne Richtlinien, Betriebsanweisungen, Sicherheits- und Arbeitsanweisungen, damit der Alltag reibungslos läuft.

Grundregeln:

- [ ] Schrank immer verschlossen halten; Schlüssel oder Zugang nur an berechtigte Personen aushändigen.
- [ ] Dokumente thematisch sortieren und nach Aufbewahrungsfrist ablegen, um Chaos und Suchzeiten zu vermeiden.
- [ ] Abgelaufene Unterlagen regelmäßig in geschützte Sammelbehälter für Aktenvernichtung überführen, um Datenschutzrisiken zu minimieren.

02 Tresor / Wertschutzschrank – Für besonders wertvolle oder kritische Inhalte.

Typische Inhalte:

- [ ] Originalurkunden wie Gründungsunterlagen, Grundbuchauszüge oder notarielle Verträge, deren Verlust rechtliche Folgen hätte.
- [ ] Unterschriftsmappen, Firmenstempel und Vollmachten, die betrieblich unverzichtbar sind.
- [ ] Datenträger mit sensiblen Informationen wie Back-up-Festplatten, USB-Sticks oder vertrauliche Projektmedien.
- [ ] Wertgegenstände wie Bargeld, Gutscheine oder sensible Hardware (z. B. Zugangstoken).

Grundregeln:

- [ ] Tresor fest verankern und in einem geschützten, unauffälligen Bereich platzieren, um Manipulationen zu erschweren.
- [ ] Zugriffsrechte klar definieren; nicht „alle Mitarbeiter mit Schlüssel“.
- [ ] Zugriffe dokumentieren, z. B. über Schließprotokolle oder Zutrittslisten, um Verantwortung nachvollziehbar zu halten.

03 Datensafe / Brandschutzschrank für Datenträger – Für hitze- und feuchtigkeitsempfindliche Medien.

Typische Inhalte:

- ☐ Backups von ERP-, HR- oder Produktionssystemen, deren Wiederherstellung im Notfall kritisch ist.
- ☐ Spezielle Datenträger wie Bänder, SSDs oder externe Festplatten, die besonders empfindlich auf Hitze und Feuchtigkeit reagieren.
- ☐ Archivierte Projektdaten, die rechtlich oder betrieblich relevant sind.

Grundregeln:

- ☐ Nur geprüfte Schränke für Datenträger verwenden (angepasste Feuer- und Temperaturklassen).
- ☐ Regelmäßige Backups nach festem Schema rotieren (täglich, wöchentlich, monatlich), um Datenverlust zu vermeiden.
- ☐ Datenträger klar beschriften (Inhalt, Datum, System) – für schnelle Wiederherstellung und Übersicht.

04 Was wird vernichtet? – Aktenvernichter & digitale Löschung richtig einsetzen.

Papierunterlagen:

- ☐ Personenbezogene Daten (Bewerbungen, alte Personalakten, Lohnlisten).
- ☐ Veraltete Verträge, Angebote oder Kalkulationen mit vertraulichen Informationen.
- ☐ Ausdrucke mit Zugangsdaten, internen Strategien oder Finanzinformationen.
- ☐ Notizen, Mitschriften und Zwischenstände, die sensible Details enthalten.

Grundregeln:

- ☐ Sicherheitsstufe passend zum Schutzbedarf wählen – höhere Stufen für Personal- und Finanzdaten.
- ☐ Sammelbehälter abschließen und regelmäßig leeren, um eine lückenlose Vernichtung sicherzustellen.

Digitale Daten:

- ☐ Veraltete Backups, die nicht mehr benötigt werden.
- ☐ Datenträger am Lebensende (defekte Festplatten, USB-Sticks, Bänder).
- ☐ Testdaten oder Kopien, die sensible Inhalte enthalten.

Tipp: Auch digital sollten Zugriffsrechte klar geregelt sein und Löschprozesse dokumentiert werden.

05 Physische Aufbewahrung + digitale Sicherung kombinieren

Grundprinzip: Wichtige Informationen werden physisch sicher aufbewahrt und digital gesichert – nie unkontrolliert doppelt verteilt.

Beispiele:

- **Wichtige Verträge:** Original im Dokumentenschrank oder Tresor, gescannte Version im revisionssicheren digitalen Archiv.
- **Kritische Betriebs- und Anlagedaten:** Arbeitsversion im System, regelmäßiges Backup in Datensafe oder Tresor.
- **Personal- und HR-Daten:** Papierunterlagen im Dokumentenschrank, digitale Akten in geschütztem System mit Rechteverwaltung.

Tipp: Physische und digitale Sicherheit ergänzen sich – so vermeiden Sie Datenverlust, Diebstahl oder versehentliche Veröffentlichung.

06

Kurzer Selbsttest für den Betrieb

- Liegen sensible Unterlagen offen auf Schreibtischen oder in Regalen?
- Sind Dokumentenschränke, Tresore und Datensafes eindeutig zugeordnet (wer hat wozu Zugriff)?
- Gibt es feste Routinen für Aktenvernichtung (z. B. monatliche „Löschrunde“)?
- Sind Backups klar beschriftet und physisch getrennt von den produktiven Systemen gelagert?

Wenn mehrere Punkte mit „Ja, aber…“ beantwortet werden:

- Strukturen prüfen, Schrank- und Tresorlösungen anpassen und klare Regeln für Aufbewahrung, Vernichtung und digitale Sicherung definieren.
- Eine kurze Schulung oder ein Reminder für Mitarbeitende kann helfen, Verantwortlichkeiten zu schärfen und Abläufe einzuhalten.