

Anlage WIV 32 – Löschkonzept für die FIT-Nordost (Vertragsanlage)

1. Geltungsbereich und Datenkategorien

Dieses Löschkonzept gilt verbindlich für alle Auftragnehmer im Rahmen des Wartungs- und Instandhaltungsvertrags der Autobahn GmbH des Bundes, Niederlassung Nordost, für die FIT-Nordost. Es definiert die Anforderungen an die sichere Löschung aller im Auftrag verarbeiteten Daten. Insbesondere sind folgende Datenarten erfasst, die im KRITIS-Umfeld der Tunnelleitzentrale anfallen können:

- Zugangsdaten (z.B. Administrator-Accounts, Passwörter)
- VPN-Informationen (Zugangsprofile, Zertifikate für Tunnelzugänge)
- Zertifikate (digitale Zertifikate für Systeme oder Nutzer)
- Logfiles (Protokolldaten von Systemen, Anwendungen und Netzwerkgeräten)
- Technische Konfigurationen (Konfigurationsdateien von Steuerungs-, Netzwerk- und Sicherheitssystemen)
- Netzwerk- und Sicherheitspläne (topologische Pläne, Sicherheitsarchitekturen, Notfallpläne)
- Personenbezogene Informationen (alle Daten, die sich auf identifizierte oder identifizierbare Personen beziehen)

All diese Daten sind entsprechend ihres Schutzbedarfs zu klassifizieren (siehe Abschnitt 2) und nach Zweckfortfall innerhalb definierter Fristen sicher zu löschen. Der Zweckfortfall ist erreicht, wenn die Daten für den ursprünglichen Verarbeitungszweck nicht mehr benötigt werden – ab diesem Zeitpunkt beginnt der Löschfristen-Zeitraum zu laufen. Gesetzliche Aufbewahrungspflichten oder anderweitige vertragliche Pflichten zur Aufbewahrung bleiben unberührt, dürfen aber die hier definierten Maximalfristen nicht überschreiten.

2. Löschfristen nach Schutzklasse

Je nach eingestufte Schutzklasse der Information gelten folgende verbindliche Löschfristen ab Zweckfortfall (Ende der Erforderlichkeit der Datenverarbeitung für den vereinbarten Zweck):

- Kritische Sicherheitsinformationen: *Löschung unverzüglich nach Zweckfortfall, spätestens innerhalb von 24 Stunden.* Diese Kategorie umfasst Informationen mit höchstem Schutzbedarf, deren Bekanntwerden gravierende Sicherheitsrisiken oder Ausfälle in der kritischen Infrastruktur verursachen könnte. Eine umgehende Vernichtung nach Nutzung ist zwingend – maximal binnen 24 Stunden.
- Streng Vertrauliche Informationen: *Löschung innerhalb von 7 Kalendertagen nach Zweckfortfall.* Darunter fallen hochsensible interne Daten, die nur einem engen Personenkreis zugänglich sind. Spätestens eine Woche nach Wegfall des Verarbeitungszwecks müssen solche Daten restlos gelöscht sein.
- Vertrauliche Informationen: *Löschung innerhalb von 30 Kalendertagen nach Zweckfortfall.* Hierzu zählen allgemeine vertrauliche Betriebs- und Sicherheitsdaten, die nicht öffentlich werden dürfen. Spätestens nach 30 Tagen sind diese Daten zu löschen.
- Personenbezogene Daten: *Löschung unverzüglich nach Zweckerreichung, spätestens innerhalb von 14 Kalendertagen.* Personenbezogene Daten sind gemäß Art. 17 DSGVO ohne ungerechtfertigte Verzögerung zu löschen, sobald sie für den Zweck nicht mehr erforderlich

sind. Im Rahmen dieses Vertrags wird eine konkrete Frist von spätestens 14 Tagen vorgegeben. Dies entspricht auch den Pflichten aus Art. 28 Abs. 3 DSGVO für Auftragsverarbeiter, wonach nach Abschluss der Verarbeitung alle personenbezogenen Daten entweder gelöscht oder an den Auftraggeber zurückgegeben werden müssen.

Die genannten Fristen sind Maximalfristen. Kürzere unternehmensinterne Vorgaben oder gesetzliche Anforderungen (z. B. sofortige Löschung bestimmter sicherheitskritischer Daten) sind vorrangig zu erfüllen. Insbesondere bei der Schutzklasse "Kritische Sicherheitsinformation" ist von einer praktisch *sofortigen* Löschung nach Gebrauch auszugehen (typischerweise unmittelbar nach Eintritt des Zweckfortfalls, dokumentiert im Löschprotokoll).

3. Zulässige Löschmethoden je Schutzklasse

Für jede Schutzklasse werden zulässige Löschmethoden vorgeschrieben, um sicherzustellen, dass Daten *endgültig und unwiederbringlich vernichtet* sind. Dabei wird zwischen digitalen Daten und physischen Datenträgern unterschieden:

a) Digitale Daten (elektronische Speichermedien): Es sind ausschließlich anerkannte, sichere Verfahren zu verwenden. Zulässig sind insbesondere:

- **Zertifizierte Löschsoftware:** Es muss Software eingesetzt werden, die nachweislich sichere Überschreib- oder Vernichtungsverfahren implementiert (z.B. gemäß BSI-Grundschutz oder internationalen Standards wie NIST SP 800-88). Solche Software (etwa Blancco oder andere zertifizierte Tools) überschreibt sämtliche Speicherbereiche und erstellt einen Nachweis der unwiderruflichen Löschung. Die Löschsoftware muss *revisionssicher* arbeiten und idealerweise von unabhängiger Stelle geprüft bzw. zertifiziert sein.
- **Kryptografische Löschung:** Bei Daten, die auf verschlüsselten Datenträgern oder in verschlüsselten Containern gespeichert sind, kann eine kryptografische Löschung erfolgen. Dabei wird der für die Entschlüsselung benötigte Schlüssel sicher und nachvollziehbar vernichtet, so dass die Daten nicht mehr lesbar sind. Dieses Crypto-Erase-Verfahren (Schlüsselvernichtung) gilt als gleichwertig zur physischen Löschung, da ohne den Schlüssel sämtliche Daten unbrauchbar werden. Dieses Vorgehen ist insbesondere bei selbstverschlüsselnden Laufwerken (SED) oder in Cloud-Umgebungen üblich.

In jedem Fall sind einfache Betriebssystem-Löschvorgänge (wie das bloße Verschieben in einen Papierkorb oder einfaches Dateilöschen) nicht ausreichend. Die eingesetzten digitalen Löschverfahren müssen den aktuellen Stand der Technik berücksichtigen und z.B. auch versteckte Sektoren oder Reservebereiche von SSDs mit einbeziehen, sofern relevant.

b) Physische Datenträger (Papierakten, Ausdrucke, Datenträger wie HDDs, SSDs, USB-Sticks, optische Medien etc.): Physische Informationsträger sind mechanisch zu vernichten nach Maßgabe der DIN 66399 (Schutzklassen und Sicherheitsstufen für die Datenträgervernichtung). Die Mindestanforderung an die Vernichtungsart richtet sich nach der höchsten darin enthaltenen Schutzklasse der Daten:

- **Datenträger mit Vertraulichen Informationen:** Vernichtung mindestens Sicherheitsstufe 2 nach DIN 66399. (Dies entspricht z.B. bei Papier einer Streifenbreite von max. 6 mm oder Partikelschnitt max. 800 mm². Sicherheitsstufe 2 ist vorgesehen für internes Schriftgut, das unlesbar gemacht werden soll.)

- Datenträger mit Streng Vertraulichen Informationen: Vernichtung mindestens Sicherheitsstufe 3 nach DIN 66399. (Dies ist das empfohlene Niveau für sensible und vertrauliche Daten. Papierdokumente etwa sind in Partikel von <320 mm² zu zerkleinern; bei elektronischen Datenträgern entspricht dies einem erhöhten Vernichtungsanspruch.)
- Datenträger mit Kritischen Sicherheitsinformationen: Vernichtung mindestens Sicherheitsstufe 4 nach DIN 66399. (Sicherheitsstufe 4 ist für *besonders sensible und vertrauliche* Daten vorgesehen. Beispiele: Papier wird dabei in Partikel <160 mm² zerschreddert; elektronische Datenträger sind mit Geräten/Verfahren zu vernichten, die dieser Stufe entsprechen – etwa durch Pulverisierung oder mehrstufige Zerkleinerung.)

Datenträger sind in geeigneter Weise *vor Ort* oder durch einen zertifizierten Dienstleister zu vernichten. Die DIN 66399 definiert insgesamt 7 Sicherheitsstufen; höhere Stufen als oben genannt können selbstverständlich ebenfalls angewendet werden, wo immer dies angebracht erscheint (eine höhere Stufe bedeutet eine noch feinere Zerkleinerung bzw. gründlichere Vernichtung). Entscheidend ist, dass das Ergebnis der Vernichtung den Anforderungen der jeweiligen Schutzklasse genügt, so dass keine Rekonstruktion der Daten möglich ist.

4. Protokollierung der Löschvorgänge

Jede Datenlöschung – unabhängig von Schutzklasse oder Verfahren – ist forensisch nachvollziehbar zu protokollieren. Das bedeutet, es muss ein Löschprotokoll geführt werden, das im Nachhinein die einwandfreie Durchführung und Vollständigkeit der Löschung belegt. Folgende Angaben sind mindestens in jedes Löschprotokoll aufzunehmen:

- Art der gelöschten Daten: Beschreibung oder Bezeichnung der Daten bzw. des Datenträgers (z. B. „Konfigurationsdatei Router XY“, „Backup-Band Nr. 5“, „Logfile vom [Datum]“, etc.).
- Zugehörige Schutzklasse: Einstufung der gelöschten Information (Kritisch, Streng Vertraulich, Vertraulich, oder personenbezogen).
- Zeitpunkt der Löschung: Datum und Uhrzeit, zu der der Löschvorgang durchgeführt wurde (ggf. Start- und Endzeitpunkt bei längeren Vorgängen).
- Verantwortliche Person: Wer die Löschung durchgeführt bzw. veranlasst hat (Name des Mitarbeiters des Auftragnehmers, ggf. mit Stellenbezeichnung).
- Angewandte Methode: Welche Löschmethode zum Einsatz kam – z.B. Name der Löschsoftware und Verfahren (Überschreiben x-fach nach Standard XY, Crypto-Erase, etc.) oder Beschreibung des physischen Vernichtungsverfahrens (z.B. Schredder nach DIN 66399 Stufe 3).

Sofern verfügbar, sind weitere Details zu dokumentieren, etwa Geräte- oder Datenträger-IDs (Seriennummern), verwendete Löschalgorithmen oder Prüfsummen. Professionelle Löschsoftware erstellt solche Protokolle automatisch und erfasst darin u.a. Datum/Uhrzeit, Operator, Gerätedaten, Löschmuster und Verifizierungsergebnisse. Diese Protokolle sind vom Auftragnehmer aufzubewahren und vor unbefugtem Zugriff geschützt zu halten. Sie dienen als Nachweis gegenüber dem Auftraggeber und ggf. Aufsichts- oder Prüfstellen, dass die Löschpflichten ordnungsgemäß erfüllt wurden.

5. Löschbestätigung und Kontrollrechte des Auftraggebers

Der Auftragnehmer ist verpflichtet, dem Auftraggeber für jede durchgeführte Löschung eine schriftliche Löschbestätigung vorzulegen. Dies kann in Form eines Löschprotokolls mit Bestätigungsschreiben oder eines formalen Löschzertifikats erfolgen. Wichtig ist, dass daraus eindeutig hervorgeht, welche Daten wann und wie gelöscht wurden und wer die Löschung vorgenommen hat. Ein solches Löschzertifikat wird bei Verwendung zertifizierter Löschsoftware in der Regel automatisch erstellt; andernfalls hat der Auftragnehmer manuell eine Bestätigung auszustellen, die den gleichen Informationsgehalt bietet.

Die Löschbestätigungen (inklusive der detaillierten Protokolle gemäß Abschnitt 4) sind dem Auftraggeber *unverzüglich* nach Durchführung der Löschung in geeigneter Form zu übermitteln. Der Auftraggeber behält sich das Recht vor, Stichprobenprüfungen der Löschprotokolle durchzuführen und die Einhaltung der Löschvorgaben im Rahmen von Audits zu überprüfen. Zu diesem Zweck hat der Auftragnehmer dem Auftraggeber auf Anforderung Einsicht in die Protokolle zu gewähren sowie ggf. weitere Informationen zum Löschvorgang zu liefern. Sollte der Auftraggeber einen externen Audit durchführen (lassen), wird der Auftragnehmer hierbei kooperieren und Zugang zu relevanten Nachweisen und Systemen gewähren, soweit dies zur Überprüfung der Lösch-Compliance erforderlich ist.

6. Verbindlichkeit und Sanktionen bei Verstößen

Die Einhaltung dieses Löschkonzepts ist verbindliche Vertragspflicht. Sämtliche hier festgelegten Vorgaben – von der Einhaltung der Löschfristen bis zur ordnungsgemäßen Durchführung und Dokumentation der Löschungen – sind vom Auftragnehmer strikt zu befolgen. Abweichungen oder Verstöße stellen einen *schwerwiegenden Vertragsverstoß* dar. Insbesondere folgende Fälle werden als gravierende Pflichtverletzung gewertet:

- Nichtrechtzeitiges Löschen von Daten nach Zweckfortfall (Überschreiten der vorgeschriebenen Frist).
- Verwendung nicht zugelassener oder unsicherer Löschmethoden, die den Anforderungen der Schutzklasse nicht genügen.
- Unterlassen der Protokollierung oder Fälschung/Unvollständigkeit von Löschnachweisen.
- Verweigerung der Auskunft oder Vorlage der Löschprotokolle gegenüber dem Auftraggeber.

Sollte ein Verstoß festgestellt werden, behält sich der Auftraggeber alle vertraglichen und gesetzlichen Sanktionsmaßnahmen vor. Dies kann je nach Schwere des Verstoßes bis zur fristlosen Kündigung des Wartungsvertrags und Schadensersatzforderungen reichen. Des Weiteren können datenschutzrechtliche Verstöße (insbesondere bei Missachtung der DSGVO-Vorgaben zur Datenlöschung) behördliche Meldungen und Bußgelder nach sich ziehen.

Der Auftragnehmer bestätigt mit Unterzeichnung des Vertrags bzw. dieser Anlage, dass er dieses Löschkonzept zur Kenntnis genommen hat und umsetzen wird. Alle Mitarbeiter des Auftragnehmers, die mit den genannten Daten in Berührung kommen, sind entsprechend zu schulen und verpflichtet, diese Vorgaben einzuhalten. Die Vertragsanlage „Löschkonzept“ ist damit integraler Bestandteil des Auftragsverhältnisses – ihre Einhaltung ist essenziell für den sicheren Betrieb der kritischen Infrastruktur FIT-Nordost und wird vom Auftraggeber ausdrücklich eingefordert.