FACTSHEET

Lösch- und Sperrkonzept in der Forderungseinziehung (Inkassounternehmen)

Dieses Factsheet ergänzt den „DS-GVO Best Practice Guide 3.0“ des BDIU um eine praxisnahe Darstellung der wesentlichen Mindestanforderungen an ein Lösch- und Sperrkonzept für Inkassounternehmen. Im Mittelpunkt steht der gesamte Lebenszyklus von Schuldner- und Forderungsdaten – von der aktiven Nutzung über die eingeschränkte Verarbeitung („Sperrung“) und Archivierung bis hin zur endgültigen Löschung – einschließlich der erforderlichen Dokumentation und operativen Umsetzung.
Das Factsheet versteht sich als praxisorientierter Orientierungsrahmen. Die konkrete Ausgestaltung des Lösch- und Sperrkonzepts ist unternehmensindividuell unter Berücksichtigung des jeweiligen Geschäftsmodells, der Systemlandschaft sowie der Risikobewertung festzulegen.

Wichtiger Hinweis:
Dieses Factsheet bezieht sich nur auf die Forderungseinziehung. Bitte denken Sie daher auch an andere Prozesse wie z.B. an Mitarbeiter- und Bewerberdaten, HR- Systeme und CRM- Systeme.

1. Zielbild und Grundprinzipien

- **Speicherbegrenzung:**
  Personenbezogene Daten sind zu löschen, sobald sie für die Zwecke der Forderungseinziehung bzw. des Forderungsmanagements oder zur Erfüllung gesetzlicher Aufbewahrungspflichten nicht mehr erforderlich sind. Maßgeblich ist eine regelmäßige Prüfung der Erforderlichkeit je Datenkategorie.
- **Nachweisfähigkeit (Rechenschaftspflicht):**
  Löschungen, Einschränkungen der Verarbeitung (Sperrungen) sowie die Ablehnung von Löschanträgen werden nachvollziehbar dokumentiert. Die Dokumentation erfolgt in der jeweiligen Forderungsakte oder in einem dafür vorgesehenen Protokollsystem.
- **Strukturierung nach Datenkategorien:**
  Personenbezogene Daten werden zu Datenkategorien zusammengefasst, z. B. Namens-, Adress-, Kommunikations-, Forderungs- oder Buchungsdaten.
  Für jede Kategorie werden verbindliche Speicherregeln (insbesondere Sperr- und Löschregeln) definiert.

Bundesverband Deutscher Inkasso-Unternehmen e.V.
Friedrichstraße 55 10117
Berlin bdiu@inkasso.de
Telefon: 030 2060736-0
Fax: 030 2060736-33

Präsidentin: Anke Blietz-Weidmann
Geschäftsführer: Dennis Stratmann
Eingetragen im Vereinsregister
AG Charlottenburg, VR 28841 B
Umsatzsteuer-ID: DE225244783

Member of FENCA www.fenca.eu

- **Systemübergreifende Anwendung:**
  Die Regeln sind für sämtliche Systeme und Speicherorte festzulegen, in denen personenbezogene Daten verarbeitet werden.

Dazu zählen neben der Inkassosoftware insbesondere Nebenablagen (z. B. Schriftverkehr, Freitextfelder, E-Mails, Dokumentenmanagement-, Ticket- oder CRM- Systeme), Archive, Backups sowie – soweit anwendbar – gespeicherte Daten bei den Auftragsverarbeitern.

2. Begriffe und Abgrenzungen

- **Löschung/ Anonymisierung:**
  Dies bezeichnet die irreversible Entfernung der personenbezogenen Daten oder des Personenbezuges aus produktiven Systemen, Archiven und sonstigen Speichermedien. Nach Durchführung dieser Maßnahmen darf ein Personenbezug weder unmittelbar noch mittelbar wiederherstellbar sein.
- **Einschränkung der Verarbeitung („Sperrung"):**
  Bei einer Sperrung verbleiben die Daten im Unternehmen, werden jedoch zur Nutzung eingeschränkt. Der Zugriff ist auf berechtigte Personen beschränkt.
  Die technische Umsetzung kann insbesondere durch entsprechende Kennzeichnung in der Forderungsakte oder im Personenstammsatz erfolgen, die eine eingeschränkte Verarbeitung systemseitig sicherstellt.
- **Archivierung:**
  Archivierung bezeichnet die technische und organisatorische Auslagerung personenbezogener Daten aus der aktiven Nutzung, insbesondere zur Erfüllung gesetzlicher Aufbewahrungspflichten oder zu Nachweiszwecken. Archivierte Daten gelten nicht als gelöscht und unterliegen weiterhin den festgelegten Speicherfristen; nach Ablauf der maßgeblichen Fristen sind sie zu löschen.

3. Geltungsbereich und Datenkategorien (Beispiele):

Das Lösch- und Sperrkonzept umfasst typischerweise folgende Datenkategorien sowie Verarbeitungsumgebungen:

- **Stammdaten:**
  Name, Anschrift, Adresshistorie, Kommunikationsdaten sowie weitere Identifikationsmerkmale.
- **Forderungs- und Verfahrensdaten:**
  Angaben zum Forderungsgrund, Forderungsstand, Titel- und Vollstreckungsdaten sowie Mahn-, Inkasso- und Prozessinformationen.
- **Kommunikationsinhalte und Nachweise:**
  Schriftverkehr, E-Mails, Telefonnotizen und sonstige Freitextdokumentationen, vom Schuldner übermittelte Unterlagen (Uploads) sowie Korrespondenz mit Bevollmächtigten.

- **Buchungs- und Zahlungsdaten:**
  Zahlungsinformationen, Kontobewegungen sowie Geschäftsbriefe und Belege mit steuer- oder handelsrechtlicher Relevanz.
- **Auskunftei- und Bonitätsdaten:**
  Bonitätsauskünfte, Adressermittlungsdaten und Unterlagen zur Identitätsprüfung.
- **IT-Umgebungen und Speicherorte:**
  Sämtliche produktiven Systeme, Test- und Schulungsumgebungen (unter Einsatz von Pseudonymisierung oder Maskierung), Fileshares, Dokumentenmanagementsysteme, Ticket- oder CRM-Systeme, E-Mail-Archive, Backups sowie Protokoll- und Logsysteme.
- **Auftragsverarbeiter und sonstige Empfänger:**
  Externe Dienstleister und Empfänger personenbezogener Daten sind im Konzept zu berücksichtigen; gegenüber Auftragsverarbeitern ist vertraglich sicherzustellen, dass Lösch- und Sperranweisungen ordnungsgemäß umgesetzt werden. Andere Empfänger personenbezogener Daten sind gegebenenfalls nachträglich über Änderungen im eigenen Datenbestand zu informieren (vgl. Art. 19 DSGVO).

4. Ab wann ist zu löschen (Auslöselogik)

Die zentrale Prüffrage für jede Datenkategorie lautet: **„Ist die Speicherung weiterhin erforderlich?“**.
Solange eine Forderung offen ist oder der Auftrag nicht abgeschlossen wurde, dürfen die erforderlichen Schuldnerdaten weiterhin verarbeitet werden. Ein Löschanspruch besteht in diesem Zeitraum regelmäßig nicht, soweit Rechtsansprüche geltend gemacht werden können.
Die folgenden Auslöser sollten im Lösch- und Sperrkonzept verbindlich definiert sein:

- **Erledigte Forderung:**
  Nach Zahlungsausgleich oder Einstellung der Forderung ist zu bestimmen, welche Daten unmittelbar gesperrt bzw. archiviert werden müssen. Maßgeblich sind dabei gesetzliche Aufbewahrungspflichten, Nachweiszwecke und ggf. das Forderungsmanagement. Ebenso ist der Zeitpunkt für die Regellöschung festzulegen.
  Bezüglich der Aufbewahrungsfristen gibt es umfangreiche Dokumente im Internet (z.B. bei der IHK). Diese können bis zu 8 Jahre sowie in Ausnahmefällen (nach § 133 InsO) bis zu 10 Jahre aufgrund von Anfechtung von Zahlungen betragen.
- **Falsche oder unzulässige Daten:**
  Fehlerhafte Daten sind zu berichtigen. Sind die alten oder unzulässigen Daten nach der Berichtigung nicht mehr erforderlich, sind sie zu löschen. Andernfalls müssen sie gesperrt und gesondert gekennzeichnet werden.
- **Reklamationen:**
  Bei substantiellen Reklamationen während der Forderungsbeitreibung kann es erforderlich sein, die betroffene Forderungsakte zu sperren.

Nach Bearbeitung der Reklamation kann die Sperre aufgehoben werden, z. B. durch Entfernung des Sperrkennzeichens.

- **Löschanträge von Betroffenen:**
  Jeder Antrag auf Löschung ist zu prüfen. Ein Anspruch auf Löschung besteht nicht, solange eine offene Forderung beigetrieben wird, soweit gesetzliche Aufbewahrungspflichten, Nachweiszwecke oder Rechtsverteidigungsgründe entgegenstehen. Entscheidungen über Löschung oder Ablehnung sind zu begründen und dem Betroffenen mitzuteilen, grundsätzlich unverzüglich bzw. spätestens innerhalb eines Monats (vgl. Art. 12 Abs. 3 DSGVO).

5. Sperrung/Einschränkung der Verarbeitung (Art. 18 DS-GVO) –

Eine Sperrung personenbezogener Daten kann in Frage kommen, wenn typische Situationen vorliegen, wie zum Beispiel:

- Die Richtigkeit der Daten wird bestritten (bis zur abschließenden Klärung).
- Ein wirksamer Widerspruch gegen die Verarbeitung auf Basis berechtigter Interessen wurde eingelegt.
- Eine Löschung wird abgelehnt, eine eingeschränkte Nutzung ist jedoch für Dokumentations- oder Nachweiszwecke erforderlich.
- Falsche oder unzulässige Daten müssen aus Nachweisgründen weiterhin vorgehalten werden (Kennzeichnung und Sperre).

Mögliche operative Maßnahmen zur Umsetzung der Sperrung:

- Gegebenenfalls Einschränkung des Betriebsablaufs.
- Zugriff nur für berechtigte Rollen („Need-to-know"), ggf. Protokollierung der Zugriffe.
- Etablierung eines Regelprozesses zur Aufhebung der Sperrung, einschließlich Entscheidung, ggf. Dokumentation sowie Fortsetzung der Verarbeitung oder Löschung.

6. Rollen, Verantwortlichkeiten und Kontrollen

- **Geschäftsführung:**
  Verabschiedet das Lösch- und Sperrkonzept, stellt die erforderlichen Ressourcen bereit und trägt die Verantwortung für die Einhaltung der Compliance-Vorgaben, einschließlich Schulungsmaßnahmen.
- **Fachbereich(e):**
  Definieren die Datenkategorien, Zwecke, Auslöser und Ausnahmen. Sie melden den Zweckfortfall, treffen Entscheidungen zu Sperr- und Löschfällen und stellen die operative Umsetzung sicher.
- **IT / Informationssicherheit:**
  Implementiert die Lösch- und Sperrlogik in allen relevanten Systemen, steuert Berechtigungen, gewährleistet Protokollierung, Backup- und Restore-Konzepte sowie die Archivierung.
- **Datenschutzbeauftragte(r):**
  Kann bei der Erstellung des Konzepts mitwirken und die Plausibilität prüfen, überwacht die Umsetzung, führt Stichproben und Audits durch und dokumentiert die Ergebnisse.

7. Systeme und Prozesse

- **Inkassosoftware und mögliche weitere Systeme bzw. Speicherorte:**
  Die eingesetzte Inkassosoftware und ggf. weitere Systeme (z.B. Dokumentenmanagement) müssen Lösch- und Sperrfunktionen bereitstellen. Die technische Konfiguration ist komplex und sollte eng mit den Softwareanbietern abgestimmt werden.
- **Manuelle Löschung:**
  Manuelle Löschvorgänge sind in Arbeitsanweisungen zu regeln, inklusive Zeitpunkt, Vorgehensweise, Ausnahmen sowie der lückenlosen Dokumentation von Löschungen und Ablehnungen in der jeweiligen Forderungsakte.
- **Backups/Wiederherstellung:**
  Das Löschkonzept muss beschreiben, wie mit Sicherungen umgegangen wird. Eine Wiederherstellung ist nur im Ausnahmefall zulässig. Die Anwendung der Löschregeln ist bei der Wiederherstellung der Daten zu beachten.

8. Dokumentation und Nachweise (Audit/Aufsicht)

- **Lösch- und Sperrregelwerk je Datenkategorie:**
  Festlegung von Regelfristen, Ausnahmen, Rechtsgrundlagen sowie Auslöser für Löschungen und Sperrungen.
- **Protokolle zu Löschung und Sperrung:**
  Dokumentation von Löschungen (inklusive Datum, Datenkategorie, Löschgrund, Methode oder Job, verantwortliche Rolle) sowie von Sperrungen (inklusive Sperrgrund und Aufhebungsdatum).
- **Dokumentation der Bearbeitung von Löschanträgen:**
  Bei Ablehnung eines Löschbegehrens ist der Akteneintrag zu begründen und die Mitteilung an den Betroffenen nachzuhalten.
- **System- und Speicherübersicht:**
  Übersicht über alle Systeme und Speicherorte, einschließlich Backups und Archive, sowie über Empfänger und Auftragsverarbeiter.
- **Regelmäßige Kontrolle:**
  Regelmäßige Überprüfung des Lösch- und Sperrkonzepts sowie stichprobenartige Wirksamkeitskontrollen zur Sicherstellung der Umsetzung.