Datenschutz und Data Warehouse

LÖSCHUNG, ANONYMISIERUNG, PSEUDONYMISIERUNG- WAS DENN NUN?

Lisa Spranz

Head of Legal | Data Protection

lisaspranz@web.de

Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Entscheidend ist allein, dass es gelingen kann, die Daten mit vertretbarem Aufwand einer bestimmten Person zuzuordnen.

Besonderen Kategorien personenbezogener Date mit automatisch höherem Schutzniveau. Zu diesen gehören genetische, biometrische und Gesundheitsdaten sowie personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit des Betroffenen hervorgehen.

Personenbezogene Daten

Name, die Telefonnummer sowie Kreditkarten- oder Personalnummern. Aber auch Kontodaten, Kfz-Kennzeichen, das Aussehen, der Gang, die Kundennummer oder die Anschrift zählen zu den personenbezogenen Daten. Selbst weniger eindeutige Informationen können einen Personenbezug ermöglichen. Beispiel EuGH Entscheidung zu Planet49 Cookie Consent

Cookie-ID und andere Online-Kennungen personenbezogenes Datum?

Ja, wenn sich über die Cookie-ID wegen der atypischen Verknüpfung mit den Registrierungsdaten der Gewinnspielteilnehmer – ein Personenbezug herstellen lässt (Rz. 45, 67 des Urteils)

Löschen im Gesetz

- Grundsatz der Datenminimierung und Speicherbegrenzung **Art. 5 Abs. 1 lit. e)** : Personenbezogenen Daten dürfen gespeichert werden, so lange wie es für die Zwecke, für die sie erhoben oder/ und verarbeitet werden, erforderlich ist.
- **Erwägungsgrund 39:** Es ist erforderlich, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt wird
- Recht auf Löschung („Recht auf Vergessenwerden“) Art. 17 Abs. 1

Datenvermeidung & Datensparsamkeit

“Soviel wie nötig, aber so wenig wie möglich“

Grundsätze der DSGVO

Art. 5 Abs.1

(a) „..in einer für die Person nachvollziehbaren Weise verarbeitet werden .. **(Transparenz)**."

(b) „..für festgelegte eindeutige und legitime Zwecke erhoben werden.. **(Zweckbindung)**."

(c) „..auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein **(Datenminimierung)**."

(d) „..damit personenbezogene Daten, die im Hinblick auf die Zwecke der Verarbeitung unrichtig sind, ..unverzüglich **gelöscht** oder **berichtigt** werden."

(f) „..**Integrität** und **Vertraulichkeit**."

Ziele

Transparenz

Nichtverkettbarkeit

Zweckbindung

Datensparsamkeit

Richtigkeit

Intervenierbarkeit

Integrität

Vertraulichkeit

Löschen und die Grundlagen

Festlegung der Speicherdauer **vor Beginn** der Verarbeitung:

Gem. **Art. 30 Abs. 1 lit. f) Verzeichnis von Verarbeitungstätigkeiten**

muss das Verzeichnis, wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien enthalten.

Informationspflichten nach **Art 13 und 14 jeweils in Abs. 2 lit. a): „zum Zeitpunkt der Erhebung“**

Plicht vom Verantwortlichen die betroffene Person über die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer zu informieren

Löschkonzept

Ein einheitliches Löschkonzept hat für die verantwortlichen Stellen folgenden Nutzen:

- Es dient dem **Schutz der Betroffenenrechte** auf Einhaltung des Datenschutzes. Die verantwortliche Stelle kann belegen, dass sie Maßnahmen definiert und umgesetzt hat, um ihren datenschutzrechtlichen Verpflichtungen zu Löschung von personenbezogenen Daten nachzukommen.
- Die Umsetzung von Löschfristen erfordert, dass die **Prozessabläufe** bis zum Ende durchdacht und geklärt werden. Unklare Prozesse müssen zwanghaft geklärt, aufwendige Abläufe unter Umständen einfacher und effizienter gestaltet werden.

Gefahr für den Betroffenen?

- Durch Erstellen von Persönlichkeitsprofilen und Vorhersagen von Verhaltens- und Handlungsweisen eines Kunden wird das informationelle Selbstbestimmungsrecht des Betroffenen tangiert. Zusätzlich werden personenbezogene Daten im Data Warehouse auf Vorrat gespeichert.
- Das Gebot der Zweckbindung soll sicherstellen, dass Daten nur für den **Zweck** verwendet werden, für den sie erhoben wurden. Eine **Änderung bzw. Erweiterung** bedarf einer **Rechtfertigung**. Eine über die Erfüllung vom ursprünglichen Zweck hinausgehende Verwendung von Daten begegnet daher grundsätzlichen Bedenken.

Löschkonzept

- Die Datenhaltung wird **systematisiert und auch konsolidiert**, da auch Altbestände in die Löschung mit einbezogen werden und damit bereinigt werden
- Durch die Bereinigung von Datenbestanden und dem Auflösen von möglichen Mehrfachdatenbeständen können **IT Betriebskosten** reduziert werden
- Die rechtlichen Vorgaben im Verzeichnis der Verarbeitungstätigkeiten bgzl. der Definition der Löschfristen werden eingehalten

Aufsichtsbehörde:

Zu empfehlende (Mindest-)Angaben im Löschkonzept:

- ✓ Betroffene personenbezogene Daten
- ✓ Verarbeitungszweck und dessen Ende
- ✓ Benennung von konkreten Ausnahmen nach Art. 17 Abs. 3 DS-GVO,
  - ❖ z.B. Aufbewahrungspflicht nach Wegfall des Verarbeitungszwecks
- ✓ Auslösendes Ereignis, ab dem die Aufbewahrungsfrist zu laufen beginnt
- ✓ Dauer der Aufbewahrungsfrist
- ✓ Datumsformel, wann die Löschung nach Ende der Aufbewahrungsfrist zu erfolgen hat
- ✓ Art und Ort der Speicherung der Daten
- ✓ Wie genau erfolgt die Löschung?

  →bei automatisierter Löschung: konkrete Beschreibung Löschvorgang
- ✓ Wer überprüft die Löschung und wie?

Löschkonzept nach DIN 66398

Der Datenbestand des Unternehmens wird in **Datenarten** aufgeteilt. Für jede Datenart wird genau eine Löschregel definiert.

Die verantwortliche Stelle sollte festlegen:

- **welche Löschregeln** für welche **Datenarten** gelten
- wie aus den Löschregeln **die Umsetzung der Löschung** erreicht wird
- wie die Löschregeln, Umsetzungsvorgaben und durchgeführten Löschmaßnahmen zu **dokumentieren** sind
- und wer für die aus dem Löschkonzept entstehenden Aufgaben der Umsetzung, Überprüfung und Fortschreibung **verantwortlich** ist.

DIN 66398 : Begriffe

- **Datenbestand:** eine Menge an personenbezogenen Daten der verantwortlichen Stellen
- **Datenart** : Gruppe von **Datenobjekten,** die zu einem **einheitlichen fachlichen Zweck** verarbeitet wird
- **Datenobjekte**: Elemente, die Daten enthalten, wie z. B. Dateien, Dokumente, Datensätze oder Attribute
- **Löschung**: Prozess, durch den pbD derart **irreversibel** verändert werden, dass sie nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können

DIN 66398 : Begriffe

- **Aufbewahrungsfrist** : Frist, für die eine Datenart nach rechtlichen Vorgaben in der verantwortlichen Stelle verfügbar sein muss
- **Regellöschfrist (Löschfrist)**: Frist, nach der eine Datenart bei regulärer Verwendung in den Prozessen der verantwortlichen Stelle spätestens zu löschen ist
- **Löschklasse**: Kombination aus einer Löschfrist und einem abstraktem Startzeitpunkt für den Fristlauf
- **Löschregel**: Kombination aus Löschfrist und konkreter Bedingung für den Startzeitpunkt des Fristlaufs
- **Standardlöschfristen**: vereinheitlichte Löschfristen für die verantwortliche Stelle
- **Vorhaltefrist**: Zeitraum, innerhalb dessen die Objekte einer Datenart in der verantwortlichen Stelle aufgrund der fachlichen Verwendung oder gesetzlicher Aufbewahrungspflichten mindestens verfügbar sein sollten

DIN 66398: Datenarten

Alle Datenbestände/ Datenobjekte, die als personenbezogene Daten eingestuft sind, müssen Datenarten zugeordnet werden!

Für jede Datenart eine Löschregel!

Datenbestände einer verantwortlichen Stelle können nach Verwendungszwecken unterschieden werden. Die Unterscheidung ergibt sich aus den einschlägigen datenschutzrechtlichen Vorschriften wie auch aus datenschutzrechtlichen Regelungen in den Spezialgesetzen..

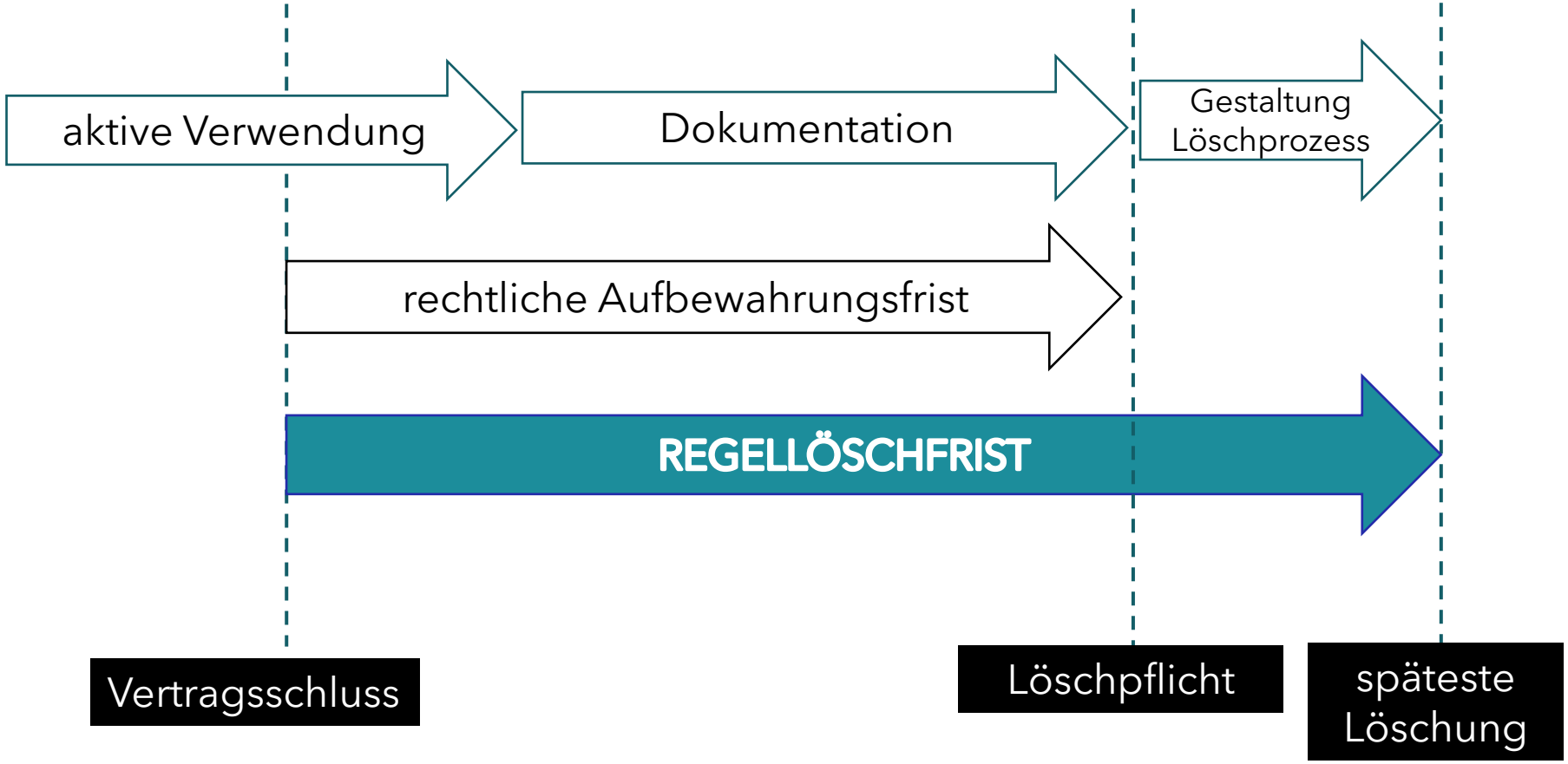
Die Zuordnung von Datenobjekten zu Datenarten ist organisationsspezifisch festzulegen, da einzelne Datenobjekte je nach verantwortlicher Stelle zu unterschiedlichen Zwecken verwendet werden können.

DIN 66398: Datenarten

Die unterschiedlichen Datenbestände werden als Datenarten bezeichnet. Unterschiedliche Zwecke und damit unterschiedliche datenarten können sich auch dann ergeben, wenn

- die relevanten datenschutzrechtlichen Vorschriften unterschiedliche Vorgaben für die Verwendung von personenbezogenen Daten treffen
- sich die Datenbestände auf unterschiedliche Betroffene beziehen
- sich die Rechtsgrundlagen für die Erhebung von Datenbeständen unterscheidet
- Datenbestände nur innerhalb eigenständiger Teilprozesse verwendet werden

Gestaltung des Löschprozesses



Aufbewahrungsfristen

3 Monate	Rechtsgrundlage
Bewerberdaten	§ 22 AGG

1 Jahr	Rechtsgrundlage
Fahrtenschreiber und Kontrollgeräte	§ 57a STVO, Art. 10 europäisches Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonal

2 Jahre	Rechtsgrundlage
Arbeitszeitnachweis (allgemein)	§ 16 Arbeitszeitgesetz
Mutterschutz	§ 19 Abs. 2 Mutterschutzgesetz
Abmahnungen	2 – 2,5 Jahre nach Rechtsprechung

Löschfristen

Weder DIN 66398 noch DSGVO legen konkreten Löschregeln und Löschfristen fest. Diese hängen maßgeblich von den zulässigen Zwecken der Verarbeitung durch die jeweilige verantwortliche Stelle ab.

Ansatz:

Standardlöschfristen empfehlen sich hier, mit einer Begrenzung auf einige wenige – zu viele Standardlöschfristen führen zu viel Komplexität.

Einschlägigen Rechtsvorschriften geben feste Fristen für die Aufbewahrung und damit der Zweckerreichung von Datenarten vor. Deren Obergrenze sollte für die Löschfrist herangezogen werden.

DIN 66398 : Löschklassen

Löschklasse: Löschfrist und abstrakter Startzeitpunkt für die Frist

Abstrakte Startzeitpunkte, ab dem der Lauf der Frist beginnt

Erhebung der personenbezogenen Daten: Die Löschfrist für ein konkretes Datenobjekt beginnt bereits bei der Erhebung durch die verantwortliche Stelle

Ende eines Vorgangs: Die Löschfrist für ein konkretes Datenobjekt beginnt erst mit dem Abschluss eines Vorgangs im Lebenszyklus des Objekts.

Ende der Beziehung zum Betroffenen: Die Löschfrist für eine konkretes Datenobjekt beginnt mit einem Ereignis, das als Ende der Beziehung zum Betroffenen definiert wird

DIN 66398 : Löschklassen

Abbildung 4: Beispiel für eine Matrix mit Löschklassen (Toll Collect)

Startzeitpunkte	Standardfristen						
	Sofort	42 Tage	120 Tage	1 Jahr	4 Jahre	7 Jahre	12 Jahre
Ab Erhebung			Mautdaten	Mautdaten mit bes. Analyse-bedarf			
Ab Ende Vorgang	nmF, Web-Logs	Kurzzeit-Doku., Betriebs-Logs	EFN, voll erstattete Reklama-tionen	Vorgänge ohne Doku-pflicht	Rekla- und Forde-rungs-daten	Handels-briefe	Buch-haltungs-daten
Ab Ende Beziehung				ergän-zende Stamm-daten		Verträge	Kern-stamm-daten.

LEGENDE:
gelb unterlegt: Frist abgeleitet aus allgemeinen Gesetzen
blau unterlegt: Frist abgeleitet aus dem Bundesfernstraßenmautgesetz
grün unterlegt: Frist frei gewählt

ABKÜRZUNGEN: nmF = Mautdaten nicht-mautpflichtiger Fahrzeuge; EFN = Einzelfahrtennachweis

Umsetzung von Löschregeln

Richtlinien können die Löschmaßnahmen für übergreifende Aspekte (Querschnittbereiche) festgelegen, z.B. Backups oder Einträge in IT-Protokollen.

Systemspezifische Umsetzungsvorgaben beschreiben die Löschmaßnahmen für alle Datenarten in einem IT-System (für IT Systeme, die nicht übergreifend sind). Die Maßnahmen könnten z. B. im jeweiligen Betriebshandbuch ergänzt werden.

Umsetzungsvorgaben können auch für manuelle Prozesse notwendig sein, z. B. als Teil von **Arbeitsanweisungen**.

Schließlich sind auch Dienstleister geeignet zu verpflichten, beispielsweise über vertragliche **Vereinbarungen im Dienstleistungsvertrag** oder AVV-Weisungen.

Löschen heisst:

Was genügt nicht, um der Löschpflicht nachzukommen?

?	Anonymisierung
×	Pseudonymisierung
×	Austragen aus Tabellen durch Löschbefehle von Betriebssystemen
×	Datenträgerformatierung
×	Freigabe von Datenträger zur Wiederverwendung (z.B. USB-Sticks)
×	Löschen des Entschlüsselungsschlüssels bei verschlüsselt gespeicherten Daten
×	Verbot der Datennutzung
×	Zusage des Verantwortlichen, die Daten nicht mehr zu verwenden

Anonym heißt also Löschen?

Ja und Nein!

Was spricht dafür?

Verschiedene Aufsichtsbehörden haben das Anonymisieren von Daten mit dem Löschen gleichgesetzt.

Ergebnis:

Für anonymisierte Datenbestände ist die DSGVO nicht gültig.

Anonym heißt Löschen

Positionspapier zur Anonymisierung des BfDI vom 29. Juni 2020:

Eine Verpflichtung zur unverzüglichen Löschung sei durch eine Anonymisierung erfüllbar.

Einschränkung: Eine Anonymisierung ist eine Verarbeitung personenbezogener Daten und folglich braucht es eine Rechtsgrundlage. Je nach Kontext und Zweck der Anonymisierung kommen (1) der Tatbestand der kompatiblen Weiterverarbeitung (Art. 6 Abs. 4 DSGVO i.V.m. der ursprünglichen Rechtsgrundlage), (2) die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 S. 1 lit. c) DSGVO) oder (3) die Einwilligung des Betroffenen (Art. 6 Abs. 1 S. 1 lit. a) DSGVO) in Betracht.

Anonymisieren und Pseudonymisieren

Die Anonymisierung verhindert, dass sich Daten bestimmten Personen zuordnen lassen. Hierfür entfernt, ersetzt, aggregiert oder verfälscht der Vorgang des Anonymisierens personenbezogene Daten oder personenbeziehbare Daten. Für vollständig anonymisierte Daten gelten bestimmte Vorgaben der DSGVO nicht.

Bei der Pseudonymisierung bleibt eine grundsätzliche Zuordnungsmöglichkeit der Daten zu bestimmten Personen bestehen. In pseudonymen Daten bleiben die Bezüge der Datensätze grundsätzlich bestehen, allerdings werden sie durch Schlüssel oder Pseudonyme für die eigentlichen Nutzer der Daten anonymisiert. Die Identifikationsmerkmale und Daten sind praktisch getrennt und der Zugang beschränkt.

Welche Stellung kommt Hash-Funktionen in der datenschutzkonformen Verarbeitung personenbezogener Daten zu?

Sind Hashfunktionen taugliche Brücken zwischen dem gesetzlich gestützten Bedürfnis nach Privatsphäre und dem berechtigten Interesse der Verwender an komplexer Datenauswertung?

Grundsatz:

Gehashte Daten sind nicht automatisch auch „anonymisierte Daten“.

Ein Personenbezug ist herstellbar, wenn auch nicht unmittelbar vorhanden.

Dies jedoch reicht wohl vollkommen aus, um auch diese Daten in den Anwendungsbereich der DSGVO fallen zu lassen.

Hashing

Auf jeden Fall:

Pseudonymisierung

Hashing ist unstrittig eine Methode der Pseudonymisierung.

Kritisch beim Daten-Handling ist vor allem die Verwendung personenbezogener Daten wie z.B. Namen, Email-Adressen, konkrete IP-Adressen oder sonstigen sogenannten „Identifiern". Hashing bedeutet, dass personenbezogene Informationen durch einen Hash in einen anderen Wert überführt werden, damit die Daten ohne den Schlüssel nicht mehr konkreten Personen zugeordnet werden können.

Das schützt zum einen direkt die Privatsphäre der User – zum anderen verhindert dies, dass personenbezogene Daten unrechtmäßig an anderer Stelle genutzt werden. Das Konzept ist im deutschen Markt schon weitgehend etabliert – allerdings ist es sinnvoll im Rahmen eines effektiven Datenschutzes noch weiter darüber hinaus zu gehen.

Hashing?

Anonymisieren?

Das kommt drauf an:

Eine Möglichkeit ist Anonymisierung durch **Drittanbieter.**

Im Idealfall wird eine Verschlüsselung über eine unabhängige dritte Partei durchgeführt, um eine mögliche Auflösung des Pseudonyms zu verhindern. Hierbei spricht man auch vom Konzept der sogenannten informationellen Gewaltenteilung, mit dem Ziel, dass keine der beteiligten Parteien Rückschlüsse auf konkrete Personen ziehen kann.

Wenn  dann Anonymisierung 

Hashing?

Eine weitere Möglichkeit ist Scrambling

Eine „Maskierung“ von Datensätzen

Hier wird der Aufbau von Datensätzen modifiziert. Ein direkter Personenbezug muss verhindert werden. Statt verschlüsselten Originaldaten kommen z.B. etwas weiter gefasste, nicht unmittelbar personenbezogene Datensegmente zum Einsatz, so dass eine Dechiffrierung grundsätzlich ausgeschlossen ist. Durch wissentlich eingeführte Fehler in den Daten ergibt sich zudem eine Verwischung, welche eine sichere Rückführung auf Personen nicht mehr zulässt und somit Daten anonym macht bzw. trotz steigender Granularität der Datenverfügbarkeit pro digitaler ID, auch anonym hält.

Diese Methodik verhindert somit effektiv eine Rückführung auf die hinter den Daten stehende Person und lässt sich via einer Durchführung über eine neutrale dritte Partei noch verstärken.

Wenn  dann Anonymisierung 

In der Praxis: Projekt „Löschkonzept"

Projektteam bilden

- Prozessverantwortlichen
- Datenschutzorganisation
- Ressourcenverantwortlichen (Vor Allem IT)

Definition der Löschregeln

- Erfassen der personenbezogenen Daten
- Gruppieren der Datenarten
- Löschklassen bilden und das Dokument „Löschregeln" erstellen
- Kontinuierliche Anpassung

Umsetzung

- Bildung von Umsetzungsvorgaben
- Festlegung von Verantwortlichen
- Dokumentation der Umsetzungsvorgaben
- Durchführen der Löschung nach den Vorgaben
- Kontinuierliche Anpassung
- Regelmäßige Prüfung der Umsetzung und Einhaltung der Vorgaben

Struktur

Erfassen der personenbezogenen Daten

- Art der Daten
- durchschnittliche Verweildauer in der Bearbeitung
- ob und wie lange die Daten aufbewahrungspflichtig sind
- ob es sich um besondere Kategorien von personenbezogenen Daten handelt
- auf welchem Datenträger diese gespeichert werden

Einwilligung

FAZIT aus Datenschutzsicht:

Umfassende Data Warehouse-Konzepte sind in der Regel nicht ohne Einwilligung des Betroffenen umsetzbar.

Haken – an die Widerrufbarkeit denken!

Fragen

Vielen Dank!