Aaron.ai

Technische und organisatorische Maßnahmen

Smarter Telefonassistent

Inhaltsverzeichnis

Stand: 22.06.2021

1. Datenminimierung

1.1 Datenvermeidung & -Löschung

Der SCA wurde mit dem Prinzip der Datensparsamkeit designt und verarbeitet nur Daten, sofern dies für die Erbringung des Dienstes erforderlich ist. Der Kunde entscheidet über die Speicherfrist und weist die Löschung an.

Betroffene	Datenkategorie	Begründung	Speicherung	Löschung
Anrufer*innen	Stimme (Audio-Daten)	Eingabemedium	Optional bei Aktivierung der Funktion durch Kunden	auf Veranlassung des Kunden
Anrufer*innen	Transkription Anliegen, zB. „Es geht um ein Rezept“	Anliegenerkennung	Ja	auf Veranlassung des Kunden
Anrufer*innen	Transkription Nachricht zB. „Ich war mit einem Infizierten in Kontakt und bitte um Rückruf“	Sprachnachricht	Ja	auf Veranlassung des Kunden
Anrufer*innen	Telefonnr.	Automatische Übermittlung / Sprachnachricht	Ja	auf Veranlassung des Kunden

1.2 Verschlüsselung

Alle personenbezogenen Daten sind im Transport verschlüsselt (TLS).

2. Verfügbarkeit

2.1 Infrastruktur

Die Aaron GmbH betreibt seine Server auf der cloudbasierten Platform-as-a-Service-Lösung von AWS, die eine hohe Verfügbarkeit garantiert.

Die gespeicherten Daten sind über verschiedene physische Server verteilt, und werden versioniert und redundant gespeichert. Zudem nutzen wir in verschiedenen Entwicklungsumgebungen unterschiedliche Datenbanken, um eine Zerstörung, Kontamination oder Verlust durch sonstige Weiterentwicklungen zu verhindern.

Der Programmcode wird über ein Versionierungssystem verwaltet, sodass jederzeit ein Rollback möglich ist.

2.2 Backup- & Recoverykonzept

Für die Einrichtung von Backup- und Recovery Systemen ist ein dedizierter Sicherheitsverantwortlicher verantwortlich.

Zur Sicherstellung der Backup-Verfügbarkeit wurde ein Recovery-Service in der Server-Administration gewählt. Der Auswahl des Service lagen die Kriterien Kapazität, Beständigkeit (99,999999999 %), Verfügbarkeit, und Sicherheitslevel zugrunde. Der Service bietet umfassende Sicherheits- und Compliance-Funktionen, z.B. werden die Daten automatisch auf mindestens drei physisch getrennte Verfügbarkeitszonen des Servers in Frankfurt verteilt, die mehrere Kilometer voneinander entfernt liegen. Die Software der Aaron GmbH ist in mehrere Dienste mit dedizierten Datenbanken unterteilt, für die mithilfe dieses Service je nach Kritikalität in angemessenen Intervallen (stündlich bis 2x wöchentlich) automatisch eine Kopie der letzten Datenstände gespeichert wird.

Durch Tests wird vor der Bereitstellung von Software sichergestellt, dass alle Funktionen fehlerfrei genutzt werden können. Die Infrastruktur wird regelmäßig getestet. Im unwahrscheinlichen Notfall, dass eine Wiederherstellung notwendig ist, startet ein Skript und lädt die zuletzt gespeicherten Daten in die jeweiligen Datenbanken.

Die Backup- und Recovery-Prozesse werden im Rahmen der halbjährlichen Audits der technisch-organisatorischen Maßnahmen der Aaron GmbH geprüft und ggf. aktualisiert.

3. Integrität

3.1 Datenkorrektur

Aufgrund des weitgehenden Verzichts auf Speicherung von personenbezogenen Daten müssen Daten nur in äußerst seltenen Ausnahmesituationen korrigiert werden. Denkbar sind allenfalls Transkriptionsfehler bei Sprachnachrichten. Auf Veranlassung des Kunden können Daten korrigiert werden.

3.2 Systemhärtung

Im Rahmen von regelmäßigen Clean-Up-Days werden nicht mehr benötigte Komponenten und Funktionen sowohl aus dem Programmcode als auch den verschiedenen Server- und Betriebsumgebungen deinstalliert und/oder entfernt.

3.3 Code-Reviews

Alle Änderungen am Programmcode werden durch Code Reviews überprüft, um Schwächen und Fehler frühzeitig zu erkennen und zu beheben. Die Änderungen werden von zwei weiteren Personen (Partner und Rollout-Manager) geprüft.

Ein automatisches Meldesystem meldet der Aaron GmbH neu erkannte Sicherheitslücken in ggf. eingesetzten Programmbibliotheken über eine zentrale Vulnerabilitätsdatenbank und führt teilweise sogar automatisch Updates durch.

3.4 Tests

Die Funktionalität aller Komponenten wird vor jedem Roll-out durch automatische und manuelle Komponenten-, Integrations- und Akzeptanztests überprüft. Das Testvorgehen ist dokumentiert und basiert auf den funktionellen Anforderungen der Software.

Zudem wird über Penetrationstests der Schutz des Systems vor Angreifern überprüft. Hinzu kommen Stress- und Lasttests sowie regelmäßige externe Tests, u.a. auch durch das BSI.

Alle Ergebnisse werden ausgewertet und Maßnahmen abgeleitet.

3.5 Berechtigungskonzept

Der Zugriff auf unsere Systeme basiert auf einem Berechtigungskonzept nach dem Erforderlichkeitsprinzip (siehe Anlage 1).

4. Vertraulichkeit

4.1 Infrastruktur

Aaron.ai unterhält selbst keine Datenverarbeitungsanlagen, sondern betreibt seine Server auf cloudbasierten Platform-as-a-Service-Lösungen. Die von uns eingesetzten Unterauftragnehmer sind zertifiziert nach ISO 27001, überwiegend auch nach C5. Die von ihnen getroffenen Sicherheitsmaßnahmen werden regelmäßig von uns und unabhängigen Prüfern überprüft.

4.2 Vertraulichkeitsvereinbarungen

Alle Mitarbeiter, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, werden auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt.

4.3 Systemhärtung

Siehe Nr. 3.2

4.4 Verschlüsselung

Siehe Nr. 1.2

4.5 Code-Reviews

Siehe Nr. 3.3

4.6 Tests

Siehe Nr. 3.4

4.7 Berechtigungskonzept

Siehe Nr. 3.5

.

5. Nichtverkettung

5.1 Zweckbindung & Datenvermeidung

Die verarbeiteten personenbezogenen Daten dürfen nur für die Bereitstellung und Erbringung des Dienstes verwendet werden. Ein Einsatz darüber hinaus ist rechtlich ausgeschlossen.

5.2 Schnittstellen

Der SCA verfügt über keine Schnittstellen zur automatischen Datenabfrage. Es existiert auch keine Download-Funktion aus der Cloud für den Kunden, die eine anderweitige Nutzung von personenbezogenen Daten vereinfachen würde.

5.3 Berechtigungskonzept

Siehe Nr. 3.5

6. Transparenz

6.1 Verarbeitungsdokumentation & Datenschutzfolgeabschätzung

Über alle Verarbeitungstätigkeiten wird ein Verarbeitungsverzeichnis angelegt und dem Kunden zur Verfügung gestellt. Da möglicherweise auch Gesundheitsdaten verarbeitet werden, wurde auch eine Datenschutzfolgeabschätzung erstellt, um das Restrisiko nach den angewandten technischen und organisatorischen Sicherheitsmaßnahmen zu prüfen. Bei Softwareupdates werden beide Dokumente aktualisiert und vom Datenschutzbeauftragten der Aaron GmbH geprüft. Bei wesentlichen Änderungen wird der Kunde informiert.

6.2 Technische Dokumentation

Die technische Dokumentation, wie z.B. die Speicherung der E-Mail-Adresse des Kundenaccounts bei Zugriffen auf die Webapplikation, wird mit dem Kunden nach jeder Änderung ausgetauscht.

6.3 Logs

Alle Verarbeitungstätigkeiten und Datenzugriffe über den Smarten Telefonassistenten oder dessen Webapplikation werden durch Logs zentral in einer Datenbank protokolliert. Dies schließt nicht nur das Nutzerverhalten, sondern auch Datenzugriffe durch den Kunden ein. Grundsätzlich erfolgt dies anonymisiert. Bei Datenzugriffen über die Webapplikation wird jedoch aus Sicherheitsgründen die IP-Adresse des Nutzers sowie die E-Mail-Adresse, die dem Kundenaccount zugeordnet ist, gespeichert. Die Daten werden nach 6 Wochen automatisch gelöscht und können nur von Administratoren eingesehen werden. Die Protokolle werden stichprobenartig vor dem Löschen überprüft.

6.4 Datenpannen

Im Falle von Datenpannen werden diese auf Basis eines standardisierten Plans nach dem Ergreifen von technischen und organisatorischen (Sofort-)Maßnahmen durch den Datenschutzbeauftragten dokumentiert und bewertet. Der Auftragsverarbeiter trifft in einem solchen Fall unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Kunden und ersucht um weitere Weisungen.

6.5 Verträge

Auftragsverarbeitungsverträge mit dem Kunden und Unterauftragsverarbeitern werden archiviert. Gleiches gilt für Vertraulichkeitsvereinbarungen mit Mitarbeitern, freien Mitarbeitern und Dienstleistern.

6.6 Betroffenenrechte

Betroffenenrechte werden dem Betroffenenkonzept (siehe Anlage 2) gemäß gewahrt.

7. Intervenierbarkeit

7.1 Vermeidung der Datenverarbeitung

Eine Nutzung von sprachgesteuerten Lösungen ohne Verarbeitung von personenbezogenen Daten (insb. der Stimme) ist grundsätzlich nicht möglich. Die Speicherung von Audioaufnahmen von Anrufenden ist optional.

7.2 Einwilligungswiderruf

Nutzer können ihre Einwilligung zur Datenverarbeitung ihm Rahmen einer Löschanfrage jederzeit widerrufen, sofern Daten gespeichert wurden. Der Kontakt erfolgt in der Regel über den Kunden. Macht ein Betroffener einen Widerruf der Einwilligung in die Datenverarbeitung unmittelbar gegenüber der Aaron GmbH geltend, verweist sie den Betroffenen unverzüglich an den Kunden und wartet dessen Weisungen ab.

7.3 Betroffenenkonzept

Bei der Bearbeitung von Betroffenenrechten wendet die Aaron GmbH ein Betroffenenkonzept an (siehe Anlage 2).

7.4 Datenkorrektur

Siehe Nr. 3.1

8. Wirksamkeitsprüfung

8.1 Verfahren

Der Datenschutzbeauftragte pflegt und aktualisiert eine Liste mit allen technischen und organisatorischen Maßnahmen. Je nach Variabilität sind manche häufiger, manche weniger häufig zu prüfen. Es ist also nötig, die Prüfmechanismen und dazugehörigen Intervalle individuell für jede getroffene Maßnahme festzulegen.

Die Aaron GmbH betreibt dazu drei verschiedene Prüfmechanismen:

- Automatische Prüfungen

- Manuelle Prüfungen
- Überprüfungen im Rahmen eines Audits

Alle Prüfungen werden unter Angabe von „wer, wann, Ergebnis“ dokumentiert und die Mitarbeiter werden im korrekten Prozess bei Abweichungen geschult.

8.2 Automatische Prüfungen

Im Rahmen automatischer Prüfungen wird täglich geprüft, ob die eingesetzte Software auf dem neusten Stand ist. Zudem werden umfangreiche Standard-Tests hinsichtlich der Belastbarkeit und der Wiedererstellbarkeit des Systems durchgeführt.

Dazu werden Logfiles nach bestimmten Textmustern gescannt, Rechner- und Gerätekonfigurationen ausgelesen und gegen einen Sollstand abgeglichen. Dabei wird nicht nur die Betriebssystemversion und das Patchlevel, sondern auch die Konfiguration der aktuellen Sicherheitseinstellungen geprüft. Dabei werden auch Tools wie Inspec verwendet, um z.B. die Rechner- und Peripheriekonfiguration automatisiert zu prüfen.

8.3 Manuelle Prüfungen

Bei Prüfungen, die nicht automatisiert durchgeführt werden können, werden regelmäßig manuell vorgenommen. Diese reichen von Stichprobenkontrollen bis zur Analyse, ob das Berechtigungskonzept noch den Anforderungen entspricht, ausgeschiedene Mitarbeiter alle Berechtigungen entzogen wurden und alle Zugriffe und Fehlfunktionen ordnungsgemäß protokolliert werden.

8.4 Audit

Alle 6 Monate wird die Konzeption der Maßnahmen insgesamt evaluiert und ggf. werden Verbesserungen implementiert. Die Aaron GmbH hat einen Sicherheitsbeauftragten benannt, der diese Prüfungen durchführt und ggf. Maßnahmen ergreift.

Zum Beispiel fällt darunter die Prüfung, ob die Sicherheit der Server weiterhin den Anforderungen entspricht, die digitalen Identitäten ergänzt werden sollten, die Authentifizierungsmethoden dem „state of the art“ entsprechen, und ob die verwendeten Rollenkonzepte überarbeitet werden müssen. Dabei werden befristete, privilegierte und administrative Berechtigungen besonders detailliert geprüft.

Zuletzt wird in diesem Rahmen festgestellt, ob einzelne Prüfaspekte weiterhin automatisiert

werden können und damit in höhere Prüfintervalle eingeordnet werden können.

Anlage 1 – Berechtigungskonzept

Erfassung aller Nutzer, Geräte und Anwendungen

Alle Informationen über Nutzer der Aaron GmbH, ihre Aufgaben und Rollen, über Geräte und Anwendungen, sowohl lokal als auch im Netzwerk und in der Cloud, werden im Rahmen von Mitarbeiterlisten, Stellenprofilen, Projektlisten, Organigrammen, Hardware-Listen, Software-Listen und Cloud-Verträge zusammengetragen. Zu diesen Nutzern ggf. auch externe Dienstleister, Kooperationspartner und Kunden.

Erstellung digitaler Identitäten

Die zu definierenden Berechtigungen werden den zugehörigen digitalen Identitäten von Nutzern, Geräten und Anwendungen zugewiesen.

Dabei wird sichergestellt, dass sich jede Person, jedes Gerät und jede Anwendung, die Zugriff auf personenbezogene Daten bekommen soll, eindeutig und sicher identifizieren lässt.

In begründeten Ausnahmefällen werden die Berechtigungen der digitalen Identität einer Nutzergruppe zugewiesen. Die Zusammensetzung der Gruppe muss dabei zu jedem Zeitpunkt nachvollziehbar sein.

Aufgliederung der Zugriffsrechte

Für jede digitale Identität wird zwischen folgenden kombinierbaren Zugriffsrechten unterschieden:

- Daten ansehen
- Neue Daten erstellen
- Daten ändern
- Daten löschen

Grundlage der Berechtigungsvergabe ist das Prinzip der minimalen Berechtigung.

Rollenkonzepte

Mehrere Nutzer, die die gleichen Aufgaben und damit die gleiche Rolle im Unternehmen haben, werden die gleichen Berechtigungen zugeordnet.

Für die Einordnung ist bei mehreren Rollen, die einer Person zugeordnet sind, die jeweils

minimale Berechtigung der maximal berechtigten Rolle maßgeblich.

Authentifizierung

Die Authentifizierung von Nutzern muss diesen Richtlinien folgen:

- Authentifizierung des Benutzers erfolgt durch Eingabe von Benutzername und Kennwort
- Benutzername und Kennwort werden gemäß den Unternehmensrichtlinien erstellt
- Die Autorisierung auf Dateien, Verzeichnisse, oder Programme erfolgt nach erfolgreicher Authentifizierung anhand der Rollenzuordnung
- Die Authentifizierung muss – ausgenommen von unter 2. genannten Ausnahmefällen - so gestaltet sein, dass ein Benutzer eindeutig identifiziert und einem Benutzerkonto zugeordnet werden kann
- Die Authentifizierung muss vor jeder anderen Interaktion zwischen System und Benutzer erfolgen
- Die Authentifizierungsinformationen müssen so gespeichert sein, dass nur autorisierte Benutzer darauf Zugriff haben

Die Administrationszugänge zu allen unsere Cloud Server sind passwortgesichert. Außerhalb des Büros ist der Zugang nur durch ein VPN mit persönlichem Schlüssel möglich.

Jeder berechtigte Mitarbeiter erhält ein eigenes Passwort, das nur ihm bekannt ist. Passwörter werden regelmäßig gewechselt und stets über einen Passwortgenerator für komplexe Passwörter mit einer Mindestlänge von 12 Stellen erzeugt.

Die Nutzung der Passwörter wird protokolliert und regelmäßig durch einen Mitarbeiter überprüft. Zugänge werden nach mehrfachen gescheiterten Anmeldeversuchen gesperrt und müssen dann durch über ein dokumentiertes Verfahren wieder freigeschaltet werden.

Alle Passwörter sowie Kryptoschlüssel werden nur verschlüsselt übertragen und verschlüsselt oder gehasht gespeichert.

Alle Mitarbeiter und Freelancer erhalten einen individuellen, passwortgesicherten VPN Zugang für Systemzugriffe. Bei kritischen Aktivitäten wie z.B. Systempflege und Backups wird nur ein internes Netzwerk genutzt und die Daten werden verschlüsselt übertragen.

Prozess Entzug/Löschung von Rechten

Arbeitet eine Person nicht länger mit den IT-Systemen, beispielsweise da der Mitarbeiter das

Unternehmen verlässt (Kündigung, Ruhestand, Zeitarbeiter, externer Dienstleister), so wird in einem definierten Verfahren sichergestellt, dass alle verbundenen Berechtigungen aus den IT-Systemen entfernt bzw. dauerhaft gesperrt werden.

Protokollierung/Monitoring der Zugriffe

Die Protokollierung aller Zugriffe erfolgt automatisch. Sie hat die Zielsetzung, den ordnungsgemäßen Betrieb zu überwachen, Fehlerzustände möglichst frühzeitig zu erkennen und den ordnungsgemäßen Umgang mit informationstechnischen Einrichtungen zu dokumentieren. Um die Nichtbeachtung des Berechtigungskonzeptes oder Manipulationsversuche zu identifizieren, werden Protokollaufzeichnungen regelmäßig auf fehlgeschlagene Anmeldeversuche überprüft.

Dokumentation

Zur Gewährleistung der Nachvollziehbarkeit und Verantwortlichkeiten bei den Zugriffsrechten, werden diese dokumentiert.

Regelmäßiger Prozess für Audit und Aktualisierung

- Die Definition und technische Umsetzung des Berechtigungskonzepts wird regelmäßig getestet und überprüft.
- Dabei werden befristete, privilegierte und administrative Berechtigungen besonders detailliert geprüft.
- Die Aaron GmbH hat einen Sicherheitsbeauftragten benannt, der diese Prüfungen durchführt und ggf. Maßnahmen ergreift.

Anlage 2 – Betroffenenkonzept

Der Kunde informiert die Nutzer seines Smarten Telefonassistenten zu Ihren Betroffenenrechten. Betroffenenrechte finden sich zudem auch auf der Website der Aaron GmbH. Der Datenschutzbeauftragte der Aaron GmbH kann unter datenschutz@aaron.ai oder unserer Postadresse mit dem Zusatz „der Datenschutzbeauftragte" erreicht werden. Wir stellen zudem sicher, dass Anfragen, die auf anderen Kanälen eingehen, innerhalb von 24 Stunden an Werktagen zur Prüfung an ihn weitergeleitet werden. Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber der Aaron GmbH geltend, verweist sie den Betroffenen unverzüglich an den Kunden und wartet dessen Weisungen ab.

Geht beim Datenschutzbeauftragten das Verlangen eines möglicherweise Betroffenen ein, wird folgender Prozess eingeleitet:

Unmittelbar:

1. Überprüfung, ob es sich um ein Verlangen bzgl. Betroffenenrechten handelt: Da in der Vergangenheit erfolgte Verlangen nicht immer eindeutig formuliert waren, prüft unser Datenschutzbeauftragter die Natur des Verlangens im ersten Schritt und ordnet diese in die Kategorien Löschanfrage, Sperranfrage, Auskunftsanfrage oder Datenkopie ein (Beispiel: Auch eine vermeintliche Kundenbeschwerde kann im Einzelfall als Auskunftsverlangen auszulegen sein. Umgekehrt stellt nicht jedes Auskunftsersuchen ein Auskunftsverlangen im datenschutzrechtlichen Sinne dar).

2. Erfassung der Anfrage in unserem CRM: Der Datenschutzbeauftragter erfasst das Verlangen inkl. der relevanten Kategorie in unserem CRM. Mit dem CRM kann die Bearbeitung, insbesondere die Einhaltung der Bearbeitungsdauer und -qualität überwacht werden. Durch eine übersichtliche Darstellung und Filterfunktion ist ein einfacher Nachweis der Beantwortung eines Auskunftsverlangens möglich.

3. Bei Betroffenenrechten wird der Kunde umgehend informiert. Optional kann die Aaron GmbH eine Eingangsbestätigung an den Antragssteller senden. Die Eingangsbestätigung informiert den Antragssteller, dass seine Anfrage eingegangen ist und macht den Prozess bis zur Beantwortung der Anfrage transparent.

4. Prüfung der Identität des Antragsstellers: Da die abgefragten Informationen zahlreiche personenbezogene Daten enthalten, muss sichergestellt sein, dass der

Antragssteller auch wirklich der Betroffene ist, dem das Auskunftsrecht zusteht. Deshalb muss vor Beantwortung der Anfrage die Identität des Antragsstellers überprüft werden. Dies erfolgt in der Regel durch einen Abgleich von mindestens zwei auf diesen Nutzer hinterlegten Datenpunkten, z.B. Kundennummer und Namen. Bei Zweifeln an der Identität des Antragsstellers oder sofern besonders geschützte Daten betroffen sind, werden weitere Informationen angefordert, die eine eindeutige Identifizierung sicherstellen.

Innerhalb von max. 2-3 Wochen: Prüfung, ob personenbezogene Daten der betroffenen Person verarbeitet wurden: Eine schnelle Überprüfung ist möglich, da bei der Aaron GmbH personenbezogene Datensätze in separaten Datenbanken vorgehalten und daher anhand der zuvor abgefragten Identifikationsmerkmale in kurzer Zeit eingesehen werden können.

Wenn keine Daten vorhanden sind: In diesem Fall wird eine Negativmitteilung an den Betroffenen versendet, d.h. es wird die Information geben, dass keine personenbezogenen Daten zu der betroffenen Person gespeichert sind.

Wenn Daten vorhanden sind: In diesem Fall unterscheidet sich der folgende Prozess je nach dem eingeforderten Betroffenenrecht.

Auskunftsverlangen & Datenkopie: In diesem Fall werden die Daten übersichtlich und automatisiert zusammengestellt. Wird der Antrag elektronisch gestellt, stellen wir die Informationen in einem gängigen elektronischen Format (z.B. PDF) bereit, andernfalls werden sie postalisch an die Absenderadresse des Betroffenen zugesendet.

Löschverlangen: In diesem Fall erfolgt eine zusätzliche Überprüfung der Berechtigung zur Löschung. Die Berechtigung wird anerkannt, wenn

- Das Speichern der Daten zur Zweckerreichung der Datenerhebung nicht mehr notwendig ist
- Der Betroffene seine Einwilligung in die Datenverarbeitung widerruft
- Die Daten unrechtmäßig verarbeitet wurden
- Die Aaron GmbH aufgrund einer gesetzlichen Pflicht zur Löschung der Daten verpflichtet ist

Ist die Berechtigung gegeben, werden die Daten anschließend gelöscht und eine Löschnotiz an den Berechtigten zugesendet (elektronisch oder postalisch). In jedem Fall wird das für das Löschverlangen angelegte Ticket im CRM anonymisiert.

Sperrverlangen: In diesem Fall erfolgt eine zusätzliche Überprüfung der Berechtigung zur

Sperrung. Die Berechtigung wird anerkannt, wenn

- der Betroffene die Richtigkeit der Daten in Frage stellt,
- die Verarbeitung unrechtmäßig ist,
- die Daten zur Geltendmachung von Rechtsansprüchen benötigt werden, nachdem der Zweck der Datenverarbeitung sich erledigt hat oder
- der Betroffene Widerspruch nach Art. 21 DSGVO eingelegt hat.

Ist die Berechtigung gegeben, werden die Daten anschließend gesperrt und eine Sperrnotiz an den Berechtigten zugesendet (elektronisch oder postalisch).

Anlage 3 – Datenflussdiagramm