

Anhang zu den Allgemeinen Geschäftsbedingungen CASAONE und Webprodukte

Auftragsdatenbearbeitungsvereinbarung (ADV) / Data Protection Agreement (DPA)

zwischen

den im Hauptvertrag genannten Kunden

(**Verantwortlicher**)

und

Casasoft AG
Thurgauerstrasse 36
CH-8050 Zürich

(**Auftragsbearbeiter**)

(zusammen: die **Parteien**)

1. Vertragsgegenstand

- (a) Der Auftragsbearbeiter bearbeitet Personendaten im Auftrag des Verantwortlichen für die Erbringung der im Vertrag zu CASAONE und/oder der Webprodukte (**Hauptvertrag**) vereinbarten Leistungen (**Dienstleistungen**). Diese Datenbearbeitung ist Gegenstand der vorliegenden Auftragsdatenbearbeitungsvereinbarung (**ADV**).
- (b) Die Parteien halten fest, dass für übergeordnete Account-Daten (meist Daten der Mitarbeitenden des Verantwortlichen zwecks Login und

Benutzermanagement des Immobilienmaklers/der Agentur) beide Parteien als separate Controller agieren. Hier sichern sie sich angemessene Unterstützung der anderen Partei zu, um allfälligen Verpflichtungen des Schweizerischen Datenschutzgesetzes nachzukommen. Diese Daten sind nicht Teil der vorliegenden Auftragsdatenbearbeitungsvereinbarung (ADV).

- (c) Gegenstand, Art und Zweck: Der Gegenstand der Datenbearbeitung, ihre Art und ihr Zweck ergeben sich aus dem Hauptvertrag. Der Auftragsbearbeiter darf die Daten ausschliesslich in anonymisierter Form für Statistiken, Produktverbesserungen und Marktanalysen verwenden.
- (d) Kreis der betroffenen Personen: Immobiliensuchende und Interessenten an Immobilienobjekten welche die Firma des Verantwortlichen zu einem aktuellen oder früheren Zeitpunkt publiziert hat, Käufer und Mieter eben dieser Objekte, interne Nutzer der CRM Applikation CASAONE und oder der Webprodukte wie Immobilienmakler und andere Mitarbeitende der Firma des Verantwortlichen, Personen die eine Geschäftsbeziehung mit dem Verantwortlichen unterhalten sowie sonstige Dritte, Webseitenbesucher der Website der Firma des Verantwortlichen.
- (e) Kategorien von Personendaten: Informationen der **Immobiliensuchenden** wie Anrede, Name, Vorname, Adresse, Telefonnummern, E-Mail Adressen sowie weitere vom Verantwortlichen optional erhobene Daten wie beispielsweise Geburtsdatum, Nationalität, Einkommen, allfällige Betreibungsregisterauszüge, Steuererklärungen, Bankauszüge oder andere Informationen über die Kreditwürdigkeit, Informationen zum Arbeitgeber oder anderen Referenzen, Pass- oder ID-Kopien, Familienstand, Kauf- oder Mietpräferenzen; Empfänger und Versender sowie Inhalte von **E-Mails** oder anderen Nachrichten, die an den Verantwortlichen gerichtet sind oder von diesem ausgehen;
Weitere Angaben zu Personen, welche eine **(Kunden-)Geschäftsbeziehung** mit dem Auftraggeber unterhalten, wie zum Beispiel beauftragte Fotografen der Immobilienobjekte oder **sonstige Dritte** wie zum Beispiel Bewohner der Immobilien zwecks Besichtigung o.ä., Stammdaten der **Auftraggeber des Verantwortlichen** wie deren Kontaktpersonen inkl. Firmenname, Jobtitel, Anrede, Name, Vorname, Adresse, Telefonnummern, E-Mail Adressen etc.; weitere Daten wie sie bei der **Nutzung von Online-Diensten** wie beispielsweise erstellter Immobilien-/Projektwebseiten anfallen wie Zugangsdaten, IP-Adressen, Geräteinformationen, Log-Dateien etc.

Die genannten Daten sind typische Beispiele, wie sie im Immobilienmakler-Tagesgeschäft des Verantwortlichen in der Anwendung der Software erhoben werden. Die im Einzelnen betroffenen Personendaten ergeben sich aus den jeweiligen Dienstleistungen bzw. aus der Nutzung durch den Verantwortlichen.

2. Definitionen

Die folgenden Begriffe haben nachstehende Bedeutungen:

- (a) **Datenschutzgesetz:** (1) Schweizer Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1) und zugehörige Verordnung (SR 235.11) bzw. ab 1. September 2023 das revidierte Schweizer Bundesgesetz über den Datenschutz und zugehörige Verordnung (gemeinsam Schweizer Datenschutzgesetz; DSG), (2) Verordnung 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Bearbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung; DSGVO), und (3) Datenschutzgesetze und -bestimmungen eines EU Mitgliedstaates oder eines anderen Landes; in der jeweils gültigen Fassung und jeweils soweit sie auf die Bearbeitung von Auftragsdaten durch den Verantwortlichen und/oder durch den Auftragsbearbeiter Anwendung finden;
- (b) **Auftragsdaten:** Personendaten, die im Auftrag des Verantwortlichen durch oder für den Auftragsbearbeiter im Zusammenhang mit dem Hauptvertrag bearbeitet werden;
- (c) **Unterauftragsbearbeiter:** Jede Person (mit Ausnahme eines Mitarbeiters des Auftragsbearbeiters oder eines seiner Unterbeauftragten), die vom Auftragsbearbeiter oder in dessen Auftrag mit der Bearbeitung von Auftragsdaten im Zusammenhang mit dem Hauptvertrag beauftragt wurde. Nicht als Unterauftragsbearbeiter gelten Anbieter von Nebenleistungen, sofern nicht systematisch auf Auftragsdaten zugegriffen wird (z.B. Wartungs- und Supportanbieter, Telekommunikations- und Postanbieter). Vorbehalten bleibt in diesen Fällen aber die Pflicht des Auftragsbearbeiters zur Gewährleistung angemessener Sicherheitsmassnahmen gemäss Ziff. 5 dieser ADV, die durch den Auftragsbearbeiter auf Anbieter von Nebenleistungen zu überbinden ist.
- (d) Die Begriffe **Verantwortlicher, betroffene Person, Mitgliedstaat,**

Personendaten (bzw. personenbezogene Daten), **Verletzung des Schutzes von Personendaten, Bearbeitung** (bzw. Verarbeitung) und **Aufsichtsbehörde** haben die diesen Begriffen in den Datenschutzgesetzen zugewiesenen Bedeutungen.

- (e) Soweit in dieser ADV nicht abweichend definiert, finden im Übrigen die Definitionen des Hauptvertrages Anwendung.

3. Stellung des Verantwortlichen

Der Verantwortliche gewährleistet, die Zulässigkeit der Erhebung, Bearbeitung und Nutzung der Auftragsdaten einschliesslich der Herstellung der erforderlichen Transparenz und der Erfüllung der gesetzlichen Betroffenenrechte (wie z.B. Auskunft, Berichtigung oder Löschung) nachweisbar sicherzustellen.

4. Pflichten des Auftragsbearbeiters

(a) Befolgung von Weisungen:

- (i) Der Verantwortliche weist den Auftragsbearbeiter an, die Daten nur in Übereinstimmung mit dem Hauptvertrag (einschliesslich dieser ADV) und dem geltenden Recht zu bearbeiten: (a) um die Dienstleistungen und technische Support Services (TSS) bereitzustellen, zu sichern und zu überwachen; und (b) wie durch (i) die Nutzung der Dienstleistungen und TSS durch den Verantwortlichen und (ii) alle anderen schriftlichen Weisungen, die vom Verantwortlichen erteilt und vom Auftragsbearbeiter als Weisungen im Rahmen dieser ADV anerkannt werden (zusammenfassend "Weisungen"), näher bestimmt. Der Auftragsbearbeiter wird den Verantwortlichen unverzüglich benachrichtigen, wenn nach Ansicht des Auftragsbearbeiters: (a) das anwendbare Recht es dem Auftragsbearbeiter verbietet, eine Weisung zu befolgen; (b) eine Weisung nicht dem anwendbaren Datenschutzrecht entspricht; oder (c) der Auftragsbearbeiter aus anderen Gründen nicht in der Lage ist, eine Weisung zu befolgen, es sei denn, eine solche Benachrichtigung ist nach anwendbarem Recht verboten.
- (ii) Sofern der Auftragsbearbeiter im Rahmen der Dienstleistungen mit den Auftragsdaten direkt interagieren kann (z.B. über eine technische

Schnittstelle zu den Systemen des Verantwortlichen), sind Weisungen grundsätzlich auf diese Art zu erteilen. Andere Weisungen sind in Textform (d.h. schriftlich, per Fax oder per E-Mail) zu erteilen, unter Vorbehalt mündlicher Weisung mit folgender Bestätigung in Textform bei Dringlichkeit.

- (b) Vertraulichkeit: Der Auftragsbearbeiter verpflichtet sich, Auftragsdaten vertraulich zu behandeln und nur Personen zugänglich zu machen, die für die Erfüllung ihrer Pflichten auf Zugang zu den Auftragsdaten angewiesen sind. Er stellt sicher, dass alle Personen mit Zugang zu Auftragsdaten einer gesetzlichen oder vertraglichen Vertraulichkeitspflicht unterstehen.
- (c) Lösch- und Rückgabepflicht:
 - (i) Wenn der Verantwortliche die Auftragsdaten nach dem Ende der Vertragslaufzeit behalten möchte, kann er den Auftragsbearbeiter während der Vertragslaufzeit anweisen, die Auftragsdaten und alle ggf. überlassenen Datenträger herauszugeben. Ansonsten sind die Auftragsdaten nach den Weisungen des Verantwortlichen und unter Vorbehalt entgegenstehender Rechtspflichten endgültig zu löschen oder wo nicht möglich zu anonymisieren.
 - (ii) Der Auftragsbearbeiter und die Unterauftragsbearbeiter sind berechtigt, Auftragsdaten nach ihren üblichen und angemessenen Prozessen in nicht produktiv genutzten Archiv- und Backup-Systemen zu speichern.

5. Datensicherheit

- (a) Sicherheitsmassnahmen: Der Auftragsbearbeiter ergreift die in Anhang 2 umschriebenen technischen und organisatorischen Massnahmen zum Schutz der Auftragsdaten (**Sicherheitsmassnahmen**) und erhält sie während der gesamten Laufzeit des Vertrags aufrecht. Der Verantwortliche hat die Sicherheitsmassnahmen geprüft und beurteilt sie als angemessen und ausreichend. Der Auftragsbearbeiter ist berechtigt, die Sicherheitsmassnahmen anzupassen, sofern das Sicherheitsniveau nicht abgesenkt wird. Anpassungen sind zu dokumentieren.
- (b) Meldung von Verletzungen: Bei Verletzungen des Schutzes der Auftragsdaten informiert der Auftragsbearbeiter den Verantwortlichen so rasch wie möglich

und in jedem Fall unter Angabe der gesetzlich erforderlichen Informationen (wobei diese Informationen auch gestaffelt übermittelt werden können, soweit sie nicht sofort bekannt sind).

6. Unterauftragsbearbeiter

- (a) Voraussetzungen: Für die Erbringung der Dienstleistungen kann der Auftragsbearbeiter Auftragsdaten an Unterauftragsbearbeiter weitergeben. Bei der Beauftragung eines Unterauftragsbearbeiters wird der Auftragsbearbeiter durch einen schriftlichen Vertrag sicherstellen, dass der Unterauftragsbearbeiter nur in dem Masse auf Auftragsdaten zugreift und diese nutzt, wie es für die Erfüllung der an ihn übertragenen Verpflichtungen erforderlich ist, und dies in Übereinstimmung mit dieser ADV geschieht.
- (b) Unterauftragsbearbeiter im Ausland: Sofern Auftragsdaten im Zusammenhang mit dem Beizug eines Unterauftragsbearbeiters in einen Staat ohne angemessenes Datenschutzniveau gelangen bzw. von dort zugänglich sind und sofern nicht der Auftraggeber mit dem Auftragsbearbeiter entsprechende Garantien vereinbart hat, ist der Auftragsbearbeiter verpflichtet und von dem Verantwortlichen ermächtigt, vor der ersten Bekanntgabe von Daten des Verantwortlichen an den betreffenden Unterauftragsbearbeiter in Übereinstimmung mit dem Datenschutzrecht geeignete Garantien vorzusehen (insb. die EU-Standardvertragsklauseln) und während der gesamten Vertragsdauer aufrechtzuerhalten.
- (c) Genehmigung: Eine Liste der bestehenden Unterauftragsbearbeiter mit Zugriff auf Auftragsdaten findet sich in Anhang 1. Vor einer Änderung der Unterauftragsbearbeitungsverhältnisse wird der Verantwortliche in Textform informiert. Erklärt er nicht innerhalb von zwei Wochen ausdrücklich und ebenfalls in Textform aus wichtigen Gründen, dass er mit der Änderung nicht einverstanden ist, gilt die betreffende Änderung als genehmigt. Falls der Verantwortliche innerhalb von zwei Wochen nach Erhalt der vorgenannten Mitteilung der Änderung in Textform widerspricht, werden die Parteien in guten Treuen eine für beide Parteien akzeptable Alternative suchen. Können sich die Parteien innerhalb von einem Monat nach Mitteilung des Widerspruchs nicht auf eine Alternative einigen, hat jede Partei das Recht, sämtliche betroffenen Dienstleistungen ohne Kostenfolgen zu kündigen. Der Auftragsbearbeiter ist in diesem Fall verpflichtet, mit den betroffenen

Auftragsdaten nach Ziff. 4(c) zu verfahren.

- (d) Haftung: Der Auftragsbearbeiter haftet dem Verantwortlichen für die Einhaltung der Pflichten der Unterauftragsbearbeiter.

7. Prüfrechte

- (a) Prüfrecht: Der Verantwortliche hat das Recht, auf eigene Kosten die Einhaltung der gesetzlichen und vertraglichen Pflichten im Zusammenhang mit der Bearbeitung von Auftragsdaten dieser ADV durch den Auftragsbearbeiter zu prüfen. Prüfungen sind nach schriftlicher Ankündigung mindestens 20 Arbeitstage im Voraus während der üblichen Geschäftszeiten und ohne unangemessene Beeinträchtigung des Geschäftsbetriebes des Auftragsbearbeiters durchzuführen. Die Parteien einigen sich im Vorfeld über Zeitpunkt, Dauer und Gegenstand der Prüfungen und über anwendbare Sicherheits- und Vertraulichkeitsbestimmungen.
- (b) Häufigkeit: Der Verantwortliche führt Prüfungen nicht öfter als einmal pro Kalenderjahr durch. Er behält aber das Recht, in begründeten Fällen – insbesondere bei Anhaltspunkten einer vertrags- oder weisungswidrigen Bearbeitung von Auftragsdaten oder einer unvorhergesehenen, wesentlichen Risikoerhöhung – weitere Prüfungen durchzuführen.
- (c) Vertraulichkeit: Der Verantwortliche behandelt die vom Auftragsbearbeiter im Rahmen einer solchen Prüfung zur Verfügung gestellten Informationen vertraulich.
- (d) Externe Prüfstelle: Der Auftragsbearbeiter hat das Recht, die Prüfung auf eigene Kosten durch eine externe, fachkundige und zur Vertraulichkeit verpflichtete Stelle durchführen zu lassen. Der Auftragsbearbeiter stellt den Prüfbericht dem Verantwortlichen zur Verfügung.

8. Kooperation

- (a) Einhaltung datenschutzrechtlicher Pflichten: Der Auftragsbearbeiter unterstützt den Verantwortlichen in angemessener Weise bei der Einhaltung datenschutzrechtlicher Pflichten.
- (b) Betroffenenrechte: Soweit ein Betroffener sich im Zusammenhang mit

datenschutzrechtlichen Ansprüchen an den Auftragsbearbeiter wendet, leitet der Auftragsbearbeiter das Begehren unverzüglich dem Verantwortlichen weiter.

- (c) Informationspflicht: Kontrollhandlungen und andere Massnahmen von Datenschutzaufsichtsbehörden sind dem Verantwortlichen ehestmöglich zu melden, wenn sie die Auftragsdaten oder die für deren Bearbeitung verwendeten Systeme betreffen.
- (d) Kostenersatz: Der Auftragsbearbeiter kann Aufwendungen, die durch die in dieser Ziff. 8 vorgesehenen Unterstützungshandlungen verursacht werden, ohne Aufschlag in Rechnung stellen, sofern sich eine entsprechende Pflicht nicht bereits aus dem Hauptvertrag ergibt. Er besitzt insofern aber kein Leistungsverweigerungsrecht.
- (e) Kontakt: Für datenschutzrechtliche Themen sind folgende Personen zu kontaktieren:

Verantwortlicher: Es sind die Kontaktpersonen des Verantwortlichen im Hauptvertrag zu kontaktieren.

Auftragsbearbeiter: dpo@casasoft.com

9. Haftung

Die Haftung der Parteien untersteht den Bestimmungen des Hauptvertrags.

10. Dauer und Beendigung

- (a) Diese ADV tritt mit ihrer Unterzeichnung oder, wenn der Hauptvertrag später abgeschlossen wird, mit Unterzeichnung des Hauptvertrags in Kraft, und endet mit der Beendigung des Hauptvertrags.
- (b) Der Verantwortliche ist zur fristlosen Kündigung dieser ADV aus wichtigem Grund berechtigt, wenn der Auftragsbearbeiter schwerwiegend gegen die Bestimmungen dieser ADV verstösst, eine vertragskonforme Weisung des Verantwortlichen nicht ausführen kann oder will oder vertragswidrig die Prüfrechte des Verantwortlichen verweigert.

11. Rangfolge der Verträge

Soweit diese Vereinbarung nichts Abweichendes vorsieht, gelten die Bestimmungen des Hauptvertrages.

12. Schlussbestimmungen

- (a) Der Verantwortliche ist berechtigt, den Hauptvertrag und/oder diese ADV mit Mitteilung in Textform mindestens 30 Tage im Voraus anzupassen, soweit dies zur Einhaltung der Datenschutzgesetze oder einer verbindlichen Anordnung einer Behörde erforderlich ist. Die Parteien bieten Hand, rechtzeitig Anpassungen dieser ADV zu verhandeln, soweit eine Anpassung der ADV nach dem vorangehenden Satz den Auftragsbearbeiter übermässig belastet.
- (b) Soweit die im Hauptvertrag vereinbarte Vergütung die Mitwirkungs- und Unterstützungspflichten nach dieser ADV durch den Auftragsbearbeiter nicht bereits abgilt, hat der Auftragsbearbeiter Anspruch auf Ersatz der dadurch konkret verursachten nachgewiesenen Kosten. Es gilt Ziff. 8(d).

1 Anhang 1: Unterauftragsbearbeiter

Informationen zum Ort		Informationen zur Datenbearbeitung
Adresse	Land	Zweck der Datenbearbeitung
SMG Swiss Marketplace Group, Werdstrasse 21, 8048 Zürich, Schweiz	Schweiz	Hosting CASAONE Filesystem (z.B. PDFs und Bilder von Immobilienobjekten)
Holycode, Jurija Gagarina 12, Beograd, Serbien	Serbien	Softwareentwicklung, Wartung als Erweiterung für unser Schweizer Entwickler-Team
Modis Contracting Solutions GmbH, Friedrichstraße 6, 70174 Stuttgart, Deutschland	Deutschland	Softwareentwicklung, Wartung mit temporären Experten für unser Schweizer Entwickler-Team
DigitalOcean, 101 6th Ave, New York, NY 10013, USA	Vereinigte Staaten (Serverstandort Frankfurt)	Hosting CASAGATEWAY (Zum Publizieren von Immobilien-Inseraten auf Portale)
Amazon Web Services, Mythenquai 10, 8002 Zürich, Schweiz	Schweiz (Serverstandort Zürich)	Hosting CASAONE CRM Software, verschlüsselt
WP Engine 504 Lavaca St #1000, Austin, TX 78701, USA	Vereinigte Staaten (Serverstandorte Belgien und Niederlande)	Hosting diverser Immobilien Webseiten und Projektwebseiten als Teil der Webprodukte von CASASOFT
Infomaniak, Infomaniak Network AG, Rue Eugène Marziano 25, 1227 Les Acacias, Schweiz	Schweiz	Backups für unsere Produkte falls die oben genannten Provider nicht mehr verfügbar sein sollten
Mandrill Mailchimp, The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000, Atlanta, GA 30308, USA	Vereinigte Staaten	Versenden von transaktionalen E-Mails wie z.B. E-Mail Notifikationen bei Verfügbarkeit von neuen Nachrichten
ActiveCampaign, 1 North Dearborn St	Vereinigte Staaten	Versenden von Marketing E-Mails zu den Produkten von CASASOFT an unsere Kunden

5th Floor Chicago, IL 60602, USA		
Aircall, 381 Park Avenue South, 16th Floor, New York, NY 10016, USA	Vereinigte Staaten	Unser Support Team nimmt Anrufe von Mitarbeitenden mittels dieser Software entgegen
Atlassian, Atlassian. Pty Ltd, Level 6, 341 George Street, Sydney NSW 2000, Australien	Australien (Datencenter in Region Europa)	Unser Support Team bearbeitet eingehende Support Tickets und E-mails mittels dieser Software.
Datadog, 620 8th Ave 45th Floor New York, NY 10018 USA	Vereinigte Staaten	System Logfile-Speicherung, System-Monitoring und Analyse
New Relic, 188 Spear Street, Suite 1000, San Francisco, CA 94105 USA	Vereinigte Staaten	System Performance Monitoring, Debugging und Analyse
Sentry, Functional Software, Inc., 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Vereinigte Staaten	System Logfile-Speicherung, System-Monitoring und Analyse

2 Anhang 2: Sicherheitsmassnahmen

Anbei die Übersicht der aktuellen Sicherheitsmassnahmen des Auftragsbearbeiters. Die Sicherheitsmassnahmen werden laufend durch Audits geprüft.

Die Technischen und Organisatorischen Massnahmen können laufend und ohne Vertragsanpassung durch den Provider angepasst werden, vorausgesetzt, dass sich das bestehende Sicherheitsniveau nicht verschlechtert.

Allfällige weitere Sicherheitsmassnahmen sind im Hauptvertrag (bzw. dessen Anhängen) geregelt.

Physische Zugangskontrolle

- 1) Definition von Sicherheitszonen
- 2) Realisierung eines effektiven, physischen Zugriffsschutzes
- 3) Definition der Personen mit physischen Zugriffsrechten
- 4) Management und Dokumentation der persönlichen Zugriffsberechtigungen über den gesamten Lebenszyklus
- 5) Begleitung von Besuchern und externem Personal
- 6) Überwachung von Räumen ausserhalb der Geschäftszeiten
- 7) Protokollierung von physischem Zugriff

Systemzugriffskontrolle

- 1) Systemzugangsschutz (Authentifizierung)
- 2) Einfache Authentifizierung von Mitarbeitenden (mittels Benutzernamen und Passwort) mit Durchsetzung eines hohen Sicherheitslevels

- 3) Zugriffsblockierung im Falle von nicht erfolgreichen Versuchen oder Inaktivität und ein Prozess um blockierte Zugriffe zurückzusetzen
- 4) Verbot des Speicherns von Passwörtern oder Formulareinträgen ausserhalb der internen Passwortmanagementlösung.
- 5) Definition der autorisierten Personen
- 6) Administration and documentation of personal authentication media and access authorizations
- 7) Automatische Blockierung des Systemzugriffs
- 8) Manuelle Blockierung des Systemzugriffs
- 9) Sicheres Übermitteln der Authentifizierungs-/Zugangsdaten im Netzwerk
- 10) Protokollierung von Systemzugriffen

Datenzugriffskontrolle

- 1) Erstellung eines Authorisierungskonzeptes
- 2) Implementierung von Datenzugriffsbeschränkungen
- 3) Standardmässiges Vergeben der minimal nötigen Zugriffsrechte
- 4) Administration und Dokumentation der Zugriffsauthorisierung für persönlichen Datenzugriff
- 5) Protokollierung von Datenzugriffen

Transport/Übermittlungskontrolle

- 1) Sichere Datenübertragung zwischen Server und Client
- 2) Sichern der Datenübertragung in den Backend-Systemen

- 3) Sichern der Datenübertragung an externe Systeme
- 4) Implementierung von Security Gateways an Netzwerkübermittlungsknoten
- 5) Hardening der Backend-Systeme
- 6) Beschreibung aller Schnittstellen und übermittelten persönlichen Datenfeldern
- 7) Machine-to-machine Authentifizierung
- 8) Datenträgermanagement (Prozedur)
- 9) Prozess für das Sammeln und Vernichten von Datenträgern
- 10) Privatsphären-orientierte Löschung und Vernichtungsprozedur

Eingabekontrolle

- 1) Dokumentation der Berechtigten für Eingaben
- 2) Logging der Einträge

Verfügbarkeitskontrolle

- 1) Backupkonzept
- 2) Business Continuity Management / Notfallplanung
- 3) Backupspeicherung
- 4) Inspektion und Prüfung der Notfallinfrastruktur

Regeln zur Funktionstrennung

- 1) Minimierte und effiziente Sammlung von Daten
- 2) Separiertes Bearbeiten der Daten

Weitere Sicherheitsbezogene Entwicklungsstandards

- 1) Vieraugenprinzip
- 2) Applikations und Repository Sicherheits-Scanning, Scanning der CI/CD Pipeline