



Katalog rechtlicher Randbedingungen

Version 1

30.11.2023

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

Allgemeine Hinweise

Dieses Dokument beschreibt Ergebnisse des Projektes „D’accord – Adaptive Datenschutz-Cockpits in digitalen Ökosystemen“ (Projektlaufzeit: 01.09.2021 bis 31.08.2024). Das Projekt wird vom Bundesministerium für Bildung und Forschung gefördert.

In D’accord werden Modelle, Konzepte und Technologien zur Umsetzung von Datenschutz-Cockpits für digitale Ökosysteme entwickelt. Den teilnehmenden Unternehmen, insbesondere KMU, ermöglicht dies, Datenschutz effektiv, rechtskonform, kostengünstig und nutzerzentriert umzusetzen. Die Nutzer werden so in die Lage versetzt, ihre Selbstbestimmungsrechte im gesamten digitalen Ökosystem wirksam auszuüben.

Konsortialpartner



HK Business Solutions GmbH

St.-Barbara-Straße 12, 66299 Friedrichsthal
Förderkennzeichen: 16KIS1506K



Fraunhofer IESE

Fraunhofer-Platz 1, 67663 Kaiserslautern
Förderkennzeichen: 16KIS1507



Hochschule Bonn-Rhein-Sieg

53754 Sankt Augustin
Förderkennzeichen: 16KIS1508



Institut für Technologie und Arbeit

Trippstadter Straße 113, 67663 Kaiserslautern
Förderkennzeichen: 16KIS1509



Universität des Saarlandes

66123 Saarbrücken
Förderkennzeichen: 16KIS1510

© D’accord-Projekt | www.daccord-projekt.de

Alle Rechte vorbehalten. Diese Veröffentlichung darf für kommerzielle Zwecke ohne vorherige schriftliche Erlaubnis des Herausgebers in keiner Weise, auch nicht auszugsweise, insbesondere elektronisch oder mechanisch, als Fotokopie oder als Aufnahme oder sonst wie vervielfältigt, gespeichert oder übertragen werden. Eine schriftliche Genehmigung ist nicht erforderlich für die Vervielfältigung oder Verteilung der Veröffentlichung von bzw. an Personen zu privaten Zwecken.

Inhaltsverzeichnis

1	Einleitung.....	6
2	Katalog rechtlicher Randbedingungen	8
2.1	Grundprinzipien des Datenschutzrechts.....	8
2.2	Betroffenenrechte	10
2.3	Pflichten des Verantwortlichen.....	13
2.4	Auftragsverarbeitung.....	20
2.5	Pflichten des Datenvermittlungsdienstes aus dem DGA.....	21

1 Einleitung

In D'accord werden technische Datenschutzlösungen in digitalen Ökosystemen betrachtet, insbesondere in Form sogenannter Datenschutz-Cockpits. Um besser nachvollziehen zu können, welche allgemeinen und speziellen **datenschutzrechtlichen Pflichten** bei der Entwicklung und dem Einsatz solcher Lösungen berücksichtigt werden müssen, wurde der nachfolgende Katalog rechtlicher Randbedingungen erstellt.

Der Ausgangspunkt der Beurteilung der Datenschutzkonformität der genannten Lösungen ist die Überprüfung der Vereinbarkeit mit den gesetzlichen Vorgaben, vornehmlich derjenigen aus der Datenschutzgrundverordnung (DSGVO) sowie denen aus datenrechtlichen Regelungen wie etwa dem Data Governance Act (DGA). Die Konkretisierung der aus diesen verschiedenen Gesetzen hervorgehenden Pflichten und Anforderungen ist essentiell, um sie für Unternehmen **besser greifbar** zu machen. Der vorliegende Katalog ist **allgemeingültig** und **wiederverwendbar**. Er stellt die Vereinbarkeit einer geplanten technischen Datenschutzlösung mit der DSGVO und dem DGA sicher.

Was sind (rechtliche) Randbedingungen?

Als **Randbedingung** wird eine Anforderung bezüglich eines Systems oder Entwicklungsprozesses bezeichnet, die den Lösungsraum über das hinaus einschränkt, was zur Erfüllung der gegebenen funktionalen und Qualitätsanforderungen notwendig ist. Eine Randbedingung beschreibt also keine Aspekte, die implementiert werden können, sondern zu befolgende Vorgaben, von denen nicht abgewichen werden kann bzw. darf.¹ Diese Vorgaben können von außen auferlegt sein, z. B. einzuhaltende Gesetze, oder organisatorische Entscheidungen sein, z. B. Entwicklung unter Berücksichtigung von gewissen Standards zur Erhalt einer Zertifizierung.

Von besonderer Relevanz für D'accord sind **rechtliche Randbedingungen**, die beim Aufbau einer digitalen Plattform bzw. der Entwicklung eines Datenschutz-Cockpits berücksichtigt werden müssen. Diese rechtlichen Randbedingungen zeichnen sich dadurch aus, dass es sich dabei mehrheitlich um verbindliche Verpflichtungen für den Adressaten handelt, die eine Voraussetzung für ein gesetzeskonformes System bilden. Entsprechend sind sie hinsichtlich ihrer Priorität als „unabdingbar“ einzustufen.

Wie wurden die Randbedingungen in D'accord beschrieben?

Da nicht alle allgemeinen und sektorspezifischen datenschutzrechtlichen Pflichten aus demselben Gesetz hervorgehen, wurde in D'accord mithilfe der rechtlichen Randbedingungen eine abstrahierte Darstellung der erwachsenden Pflichten vorgenommen. Die Randbedingungen sind organisiert in **fünf Oberkategorien**: Betroffenenreche, Grundprinzipien des Datenschutzrechts, Pflichten des Verantwortlichen, Auftragsverarbeitung und Pflichten des Datenvermittlungsdienstes aus dem DGA.

Zur Formulierung der Randbedingungen wurden **Satzschablonen** verwendet, wie sie häufig im Requirements Engineering anzufinden sind,² mit Varianten für Anforderungen ohne

¹ Martin Glinz: A Glossary of Requirements Engineering Terminology (Version 2.0.1). International Requirements Engineering Board. 2022.

² Chris Rupp/SOPHISTen: Requirements Engineering und -Management, 6. Auflage, Hanser Verlag, München, 2020.

Vorbedingung („*Der Verantwortliche muss...*“) bzw. mit Vorbedingung („*Wenn [Bedingung], muss der Verantwortliche...*“). Das Wort „muss“ impliziert hierbei immer eine gesetzliche Verpflichtung mit der **Priorität** „unabdingbar“. Zur Differenzierung der Randbedingungen wurde untersucht, ob der Grad, mit dem die Anforderung umgesetzt werden kann (**“Impact“**), bestimmt werden kann.

Jede Randbedingung besteht aus einem **Namen**, einer **Beschreibung**, einem Verweis zu der jeweiligen **Rechtsgrundlage**, der **Intention** des Gesetzgebers hinter der jeweiligen Anforderung („Der Gesetzgeber will damit erreichen, dass...“) sowie einer Betrachtung, ob die Erfüllung der Randbedingung über eine **Nutzerinteraktion** erfolgt (z. B. Bereitstellung von Informationen) oder nicht (z. B. Vorgaben an die Verarbeitung).

2 Katalog rechtlicher Randbedingungen

2.1 Grundprinzipien des Datenschutzrechts

Name	Verarbeitung in einer rechtmäßigen Weise und nach Treu und Glauben
Beschreibung	Der Verantwortliche muss Daten in einer rechtmäßigen Weise und nach Treu und Glauben verarbeiten.
Intention	Der Gesetzgeber möchte, dass Verantwortliche bei der Verarbeitung personenbezogener Daten die Grundsätze der DSGVO und anderer einschlägiger Gesetze einhält und dabei nicht gegen grundlegende Wertevorstellungen verstößt.
Rechtsgrundlagen	Art. 5 Abs. 1 lit. a DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerrückmeldung	nein

Name	Zweckbindung
Beschreibung	Der Verantwortliche darf Daten nur für festgelegte, eindeutige und legitime Zwecke erheben und muss sicherstellen, dass die Daten nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
Intention	Der Gesetzgeber möchte, dass Verantwortliche personenbezogene Daten nur zu angemessenen und legitimen Zwecken verarbeiten.
Rechtsgrundlagen	Art. 5 Abs. 1 lit. b DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerrückmeldung	nein

Name	Datenminimierung
Beschreibung	Der Verantwortliche muss sicherstellen, dass er nur so viele Daten, wie für den Zweck unbedingt notwendig, verarbeitet werden.
Intention	Der Gesetzgeber möchte, dass Verantwortliche möglichst wenige Daten erheben und nur die Daten, die wirklich notwendig sind.
Rechtsgrundlagen	Art. 5 Abs. 1 lit. c DSGVO

Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerrinteraktion	nein

Name	Richtigkeit
Beschreibung	<p>Der Verantwortliche muss sicherstellen, dass er nur Daten verarbeitet, die sachlich richtig und auf dem neuesten Stand sind.</p> <p>Der Verantwortliche muss alle angemessenen Maßnahmen ergreifen, die notwendig sind um sicherzustellen zu können, dass personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.</p>
Intention	Der Gesetzgeber möchte, dass Verantwortliche nur Daten verarbeiten, die sachlich richtig sind, damit keine Nachteile für betroffene Personen entstehen.
Rechtsgrundlagen	Art. 5 Abs. 1 lit. d DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerrinteraktion	nein

Name	Speicherbegrenzung
Beschreibung	<p>Der Verantwortliche muss sicherstellen, dass er Daten nur so lange aufbewahrt, wie es für den Zweck der Verarbeitung wirklich erforderlich ist.</p> <p>Wenn einer der Lösungsgründe nach Art. 17 DSGVO vorliegt, muss der Verantwortliche die Daten löschen.</p>
Intention	Der Gesetzgeber möchte, dass betroffene Personen wissen, welche ihrer Daten wie lange gespeichert werden. Hilfreich ist es auch, wenn die betroffenen Personen Lösungskonzepte/-intervalle kennen.
Rechtsgrundlagen	Art. 13 Abs. 2 lit. a DSGVO; Art. 5 Abs. 1 lit. e DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerrinteraktion	nein

Name	Integrität und Vertraulichkeit
Beschreibung	Der Verantwortliche muss die Sicherheit der Daten, die verarbeitet werden, gewährleisten. Der Verantwortliche und der Auftragsverarbeiter müssen für die Gewährleistung der Datensicherheit geeignete technische und organisatorische Maßnahmen ergreifen.
Intention	Der Gesetzgeber möchte, dass Verantwortliche personenbezogene Daten auch in technischer Hinsicht sichern, insbesondere auch gegen Angriffe von außen.
Rechtsgrundlagen	Art. 5 Abs. 2 lit. f DSGVO, Art. 24, 25, 28 Abs. 3 S. 2 lit. c, 32 DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

2.2 Betroffenenrechte

Name	Einrichtung zur Geltendmachung von Betroffenenrechten
Beschreibung	Der Verantwortliche muss die betroffene Person aktiv dabei unterstützen, ihre Betroffenenrechte geltend zu machen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen ihre Rechte möglichst einfach geltend machen können und ihnen alle notwendigen Informationen zur Verfügung stehen.
Rechtsgrundlagen	Art. 12 Abs. 2 S. 1 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Recht auf Auskunft
Beschreibung	Wenn Daten einer betroffenen Person verarbeitet werden, muss der Verantwortliche den betroffenen Personen hierüber Auskunft erteilen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen wissen, wer welche ihrer Daten verarbeitet.
Rechtsgrundlagen	Art. 15 DSGVO, Art. 12 Abs. 1 und 2 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits

Erfordert eine Nutzerinteraktion	ja
---	----

Name	Recht auf Berichtigung/Ergänzung
Beschreibung	Wenn Daten einer betroffenen Person unrichtig oder unvollständig sind, muss der Verantwortliche diese korrigieren oder vervollständigen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen falsche oder unvollständige Daten möglichst einfach korrigieren lassen können.
Rechtsgrundlagen	Art. 16 DSGVO, Art. 12 Abs. 1 und 2 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Recht auf Löschung
Beschreibung	Wenn ein Lösungsgrund aus Art. 17 DSGVO vorliegt, muss der Verantwortliche die entsprechenden Daten der betroffenen Person löschen.
Intention	Der Gesetzgeber möchte, dass Verantwortliche personenbezogene Daten löschen, soweit sie nicht mehr benötigt werden. Ferner möchte der Gesetzgeber, dass betroffene Personen die Löschung beantragen können, wenn die Löschung nicht automatisch erfolgt.
Rechtsgrundlagen	Art. 17 DSGVO, Art. 12 Abs. 1 und 2 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Recht auf Einschränkung der Verarbeitung
Beschreibung	Wenn eine der Voraussetzungen aus Art. 18 Abs. 1 lit. a - d DSGVO gegeben ist, muss der Verantwortliche in verschiedenen Situationen die Verarbeitung einschränken.
Intention	Der Gesetzgeber möchte, dass betroffene Personen in verschiedenen Situationen die Verarbeitung einschränken können, bspw. wenn die Verarbeitung unrechtmäßig ist, aber eine Löschung nicht in Frage kommt.

Rechtsgrundlagen	Art. 18 DSGVO, Art. 12 Abs. 1 und 2 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Recht auf Datenübertragbarkeit
Beschreibung	Der Verantwortliche muss der betroffenen Person oder einem anderen Verantwortlichen Daten in einem gängigen und strukturierten maschinenlesbaren Format zukommen lassen.
Intention	Der Gesetzgeber möchte, dass betroffene Person ihre Daten ggf. möglichst einfach anderen Verantwortlichen zukommen lassen können. Dafür müssen die Daten in einem gängigen und strukturierten maschinenlesbaren Format geteilt werden. Hierdurch wird der Übergang von einem zum anderen Verantwortlichen erleichtert.
Rechtsgrundlagen	Art. 20 DSGVO, Art. 12 Abs. 1 und 2 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Recht auf Auskunft
Beschreibung	Wenn Daten einer betroffenen Person verarbeitet werden, muss der Verantwortliche sie darüber informieren.
Intention	Der Gesetzgeber möchte, dass betroffene Personen wissen, wer welche ihrer Daten verarbeitet.
Rechtsgrundlagen	Art. 15 DSGVO, Art. 12 Abs. 1 und 2 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

2.3 Pflichten des Verantwortlichen

Name	Informationen zum Verantwortlichen mit Kontaktdaten
Beschreibung	Der Verantwortliche muss der betroffenen Person Kontaktdaten zu sich selbst und zu einer Kontaktstelle zur Verfügung stellen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen klare Angaben zum Verantwortlichen erhalten und somit eine Ansprechperson zur Geltendmachung von Betroffenenrechten kontaktieren können.
Rechtsgrundlagen	Art. 12, 13 Abs. 1 lit. a, Art. 5 Abs. 1 lit. a DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Aufklärung über alle durchgeführten Datenverarbeitungen
Beschreibung	Der Verantwortliche muss betroffene Personen hinreichend über alle vorgenommenen Datenverarbeitungen aufklären.
Intention	Der Gesetzgeber möchte, dass betroffene Personen überblicken können, welche Verarbeitungen ihrer personenbezogenen Daten durchgeführt werden.
Rechtsgrundlagen	Art. 5 Abs. 1 lit. a DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Aufklärung über alle Zwecke, zu denen die Datenverarbeitung durchgeführt wird
Beschreibung	Der Verantwortliche muss betroffene Personen hinreichend über die Zwecke der Datenverarbeitung aufklären.
Intention	Der Gesetzgeber möchte, dass betroffene Personen die Zwecke der Verarbeitung ihrer personenbezogenen Daten kennen.
Rechtsgrundlagen	Art. 13 Abs. 1 lit. c DSGVO, Art. 5 Abs. 1 lit. a und b DSGVO Art. 12 lit. a DGA
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits

Erfordert eine Nutzerinteraktion	ja
---	----

Name	Aufklärung über Zweckänderungen
Beschreibung	Wenn der Verarbeitungszweck sich ändert, muss der Verantwortliche die betroffene Person über die neuen Zwecke informieren. Soll eine Zweckänderung nach Art. 6 Abs. 4 DSGVO durchgeführt werden, ist eine Kompatibilitätsprüfung des alten mit dem neuen Zweck durchzuführen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen Änderungen des Zwecks angezeigt bekommen und sie ggf. reagieren oder ihre Einwilligung verweigern können. Ferner möchte der Gesetzgeber, dass Verantwortlichen die Daten nicht für andere als die von den betroffenen Personen akzeptierten bzw. ihnen mitgeteilten Zwecke verarbeitet werden. Der Verantwortliche muss die Datenverarbeitung auf das absolut notwendige Maß beschränken.
Rechtsgrundlagen	Art. 13 Abs. 1 lit. c DSGVO, Art. 5 Abs. 1 lit. a, b und c, Art. 6 Abs. 4 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Aufklärung über mögliche Übermittlungen von Daten
Beschreibung	Wenn Daten an eine andere Institution übermittelt werden, muss der Verantwortliche dies der betroffenen Person mitteilen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen wissen, an wen ihre Daten übermittelt werden.
Rechtsgrundlagen	Art. 13 Abs. 1 lit. e DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Aufklärung über mögliche Drittlandsübermittlungen
Beschreibung	Wenn Daten in Drittländer übermittelt werden, muss der Verantwortliche offenlegen, in welche Drittländer und aufgrund welcher Rechtsgrundlage (z. B. Angemessenheitsbeschluss). Wenn kein

	Angemessenheitsbeschluss vorliegt, muss der Verantwortliche dies explizit aufzeigen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen wissen, ob ihre Daten in Drittländer übermittelt werden.
Rechtsgrundlagen	Art. 13 Abs. 1 lit. f DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Mitteilung des Datenschutzbeauftragten an die betroffene Person
Beschreibung	Der Verantwortliche muss den betroffenen Personen seinen Datenschutzbeauftragten mitteilen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen einen Ansprechpartner beim Verantwortlichen haben. Hierfür ist die Mitteilung des Datenschutzbeauftragten wichtig.
Rechtsgrundlagen	Art. 13 Abs. 1 lit. b DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Beschwerderecht
Beschreibung	Der Verantwortliche muss die betroffenen Personen über die Möglichkeit des Beschwerderechts informieren.
Intention	Der Gesetzgeber möchte, dass betroffene Personen die Möglichkeit, sich bei einer Aufsichtsbehörde zu beschweren, kennen.
Rechtsgrundlagen	Art. 13 Abs. 2 lit. d DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Aufklärung über die der Verarbeitung zugrundeliegenden Rechtsgrundlage
Beschreibung	Der Verantwortliche muss die betroffenen Personen über die Rechtsgrundlage der Verarbeitung informieren.

Intention	Der Gesetzgeber möchte, dass betroffene Personen die Rechtsgrundlage der Verarbeitung kennen.
Rechtsgrundlagen	Art. 13 Abs. 1 lit. c DSGVO, Art. 5 Abs. 1 lit. a DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Aufklärungen in einfacher und verständlicher Sprache
Beschreibung	Der Verantwortliche muss die Informationen über Datenverarbeitungen in möglichst einfacher und verständlicher Form und in einfacher und klarer Sprache erteilen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen eine möglichst übersichtliche und einfach verständliche Aufklärung über Datenverarbeitungen erhalten.
Rechtsgrundlagen	Art. 12 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

Name	Zugänglichkeit zu allen erforderlichen Informationen
Beschreibung	Der Verantwortliche muss den Zugang zu Informationen für die betroffene Person möglichst einfach gestalten.
Intention	Der Gesetzgeber möchte, dass betroffene Personen einfach Zugang zu Informationen zu durchgeführten Datenverarbeitungen haben und sie diese nicht lange suchen müssen.
Rechtsgrundlagen	Art. 12 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

Name	Vollständig automatisierte Einzelfallentscheidungen
Beschreibung	Wenn eine Entscheidung des Verantwortlichen vollständig auf einer automatisierten Datenverarbeitung beruht, muss der Verantwortliche dies der betroffenen Person mitteilen. Solche vollständig auf

	automatisierten Datenverarbeitungen beruhenden Entscheidungen sind verboten, soweit sie der betroffenen Person gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen wissen, ob eine sie betreffende Entscheidung vollständig automatisiert oder mithilfe von menschlichen Zwischenschritten getroffen wird, sodass sie ggf. reagieren und widersprechen können.
Rechtsgrundlagen	Art. 13 Abs. 2 lit. f DSGVO; Art. 22 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Auskunftsanspruch u.a. bei vollständig automatisierten Einzelfallentscheidungen
Beschreibung	Der Verantwortliche ist dazu verpflichtet, aussagekräftige Informationen über vorhandene Daten und die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu erteilen.
Intention	Der Gesetzgeber möchte, dass betroffene Personen wissen, wie der Algorithmus bei einer vollständig automatisierten Einzelentscheidung funktioniert.
Rechtsgrundlagen	Art. 13 Abs. 2 lit. f DSGVO; Art. 22 DSGVO, Art. 15 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Rechenschaftspflicht
Beschreibung	Der Verantwortliche muss nachweisen können, dass er die grundlegenden Prinzipien des Datenschutzrechtes (Art. 5 Abs. 1 DSGVO) eingehalten hat. Hierfür ist beispielsweise ein Verarbeitungsverzeichnis (Art. 30 DSGVO) erforderlich.
Intention	Der Gesetzgeber möchte, dass Verantwortliche grundlegende Prinzipien bei der Datenverarbeitung einhalten. Ferner möchte der Gesetzgeber betroffene Personen dadurch entlasten, dass der Verantwortliche grundsätzlich in der Nachweispflicht für die Einhaltung dieser Prinzipien ist.

Rechtsgrundlagen	Art. 5 Abs. 2 DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerrinteraktion	nein

Name	Nachweis der Ergreifung angemessener technischer und organisatorischer Maßnahmen
Beschreibung	Der Verantwortliche muss nachweisen können, dass er zur Sicherstellung der Sicherheit der Verarbeitung geeignete technische und organisatorische Maßnahmen ergreift.
Intention	Der Gesetzgeber möchte, dass Verantwortliche personenbezogene Daten auch in technischer Hinsicht sichern, insbesondere auch gegen Angriffe von außen. Ferner ist es dem Gesetzgeber wichtig, dass betroffene Personen nicht selbst Verstöße beweisen müssen, sondern der Verantwortliche in der Pflicht ist.
Rechtsgrundlagen	Art. 24 Abs. 1 S. 1 DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerrinteraktion	nein

Name	Meldepflicht gegenüber betroffenen Personen bei Verletzungen des Schutzes personenbezogener Daten
Beschreibung	Wenn aus Sicht des Verantwortlichen nach Durchführung einer Prognoseentscheidung hinsichtlich der möglichen Folgen der Datenpanne ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zu erwarten ist, muss der Verantwortliche dies unverzüglich den betroffenen Personen melden. Sinnvoll ist in diesem Zusammenhang die Führung eines Konzepts, welches im Falle einer Datenpanne angewendet werden kann.
Intention	Der Gesetzgeber möchte, dass betroffene Personen im Falle einer Datenpanne informiert werden, wenn durch die Datenpanne ein hohes Risiko für ihre persönlichen Rechte und Freiheiten entsteht.
Rechtsgrundlagen	Art. 34 Abs. 1 DSGVO
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerrinteraktion	ja

Hinweise	Die RAB 33 betrifft nur die Meldepflicht des Verantwortlichen, die nach erfolgter Prognoseentscheidung im Sinne des Art. 34 DSGVO greift.
-----------------	---

Name	Meldepflicht gegenüber der Aufsichtsbehörde bei Verletzungen des Schutzes personenbezogener Daten
Beschreibung	Wenn eine Verletzung des Schutzes personenbezogener Daten festgestellt wird, muss der Verantwortliche dies unverzüglich und möglichst binnen 72h der zuständigen Aufsichtsbehörde melden.
Intention	Der Gesetzgeber möchte die effektive Überwachung durch die Aufsichtsbehörden sicherstellen.
Rechtsgrundlagen	Art. 33 DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzereinteraktion	nein

Name	Gemeinsame Verantwortlichkeit
Beschreibung	Wenn eine gemeinsame Verantwortlichkeit für die Datenverarbeitung anzunehmen ist, müssen die gemeinsam Verantwortlichen einen Joint-Controller-Vertrag im Sinne des Art. 26 DSGVO abschließen, der die tatsächlichen Beziehungen und Funktionalitäten beider Beteiligten zeigt.
Intention	Der Gesetzgeber möchte, dass betroffene Personen wissen, wem die Datenverarbeitung zuzurechnen ist und an wen sie sich wenden müssen/können.
Rechtsgrundlagen	Art. 26 DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzereinteraktion	nein

2.4 Auftragsverarbeitung

Name	Weisungsgebundenheit des Auftragsverarbeiters
Beschreibung	<p>Der Auftragsverarbeiter muss die Anweisungen des Verantwortlichen befolgen (weisungsgebunden) und darf diese nicht überschreiten.</p> <p>Der Auftragsverarbeiter muss sicherstellen, dass er nur auf dokumentierte Weisung des Verantwortlichen handelt.</p>
Intention	Der Gesetzgeber möchte, dass die Zuständigkeiten bei der Verarbeitung personenbezogener Daten klar verteilt sind. Hierzu gehört auch, dass der Auftragsverarbeiter, dem die Verarbeitung nicht zuzurechnen ist, nur in den Grenzen des durch den Verantwortlichen Erlaubten handelt.
Rechtsgrundlagen	Art. 28 Abs. 3 S. 2 lit. a DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

Name	Auftragsverarbeitungsvertrag
Beschreibung	Der Verantwortliche muss einen Auftragsverarbeitungsvertrag im Sinne des Art. 28 DSGVO mit seinen Auftragsverarbeitern abschließen. Die Mindestinhalte ergeben sich aus Art. 28 Abs. 3 DSGVO.
Intention	Der Gesetzgeber möchte, dass betroffene Personen wissen, wem die Datenverarbeitung zuzurechnen ist, wer sie durchführt und an wen sie sich wenden müssen/können.
Rechtsgrundlagen	Art. 28 DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

2.5 Pflichten des Datenvermittlungsdienstes aus dem DGA

Name	Anmeldung des Datenvermittlungsdienstes
Beschreibung	Der Anbieter eines Datenvermittlungsdienstes im Sinne des Art. 10 DGA muss den Dienst nach Art. 11 Abs. 1 DGA bei der zuständigen Behörde anmelden.
Intention	Der Gesetzgeber möchte, dass ein Anmeldeverfahren für Datenvermittlungsdienste eingeführt wird, damit sichergestellt ist, dass die Daten-Governance auf der Grundlage einer vertrauenswürdigen Datenweitergabe in der Union erfolgt.
Rechtsgrundlagen	Art. 11 Abs. 1, 10 lit. b DGA Inhalt der Anmeldung: Art. 11 Abs. 6 DGA
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

Name	Zweckbindung
Beschreibung	Der Anbieter des Datenvermittlungsdienstes muss die strenge Zweckbindung, die der DGA normiert, einhalten; die Daten dürfen zu keinem anderen Zweck als der Bereitstellung für Datennutzer verarbeitet werden.
Intention	Der Gesetzgeber möchte, dass Datenvermittlungsdienste als neutrale Datenmittler tätig werden. Daher dürfen die Datenvermittlungsdienste die bereitgestellten Daten nur zum Zwecke der Bereitstellung für Datennutzer verwenden.
Rechtsgrundlagen	Art. 12 lit. a DGA; Art. 5 Abs. 1 lit. b DSGVO
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

Name	Kommerzielle Bedingungen und Preisgestaltung
Beschreibung	Der Anbieter des Datenvermittlungsdienstes muss sicherstellen, dass kommerzielle Bedingungen und Preisgestaltung nicht davon abhängig sind, ob und in welchem Umfang der Dateninhaber oder Datennutzer Dienste desselben Anbieters nutzen.

Intention	Der Gesetzgeber möchte, dass eine strukturelle Trennung des Datenvermittlungsdienstes von allen anderen erbrachten Diensten, vorgenommen wird, um Interessenkonflikte zu vermeiden.
Rechtsgrundlagen	Art. 12 lit. b DGA
Impact auf das Projekt	Out of Scope
Erfordert eine Nutzerinteraktion	nein

Name	Daten zur Erbringung des Datenvermittlungsdienstes
Beschreibung	<p>Der Anbieter des Datenvermittlungsdienstes darf Daten, die in Bezug auf Tätigkeiten einer natürlichen oder juristischen Person zur Erbringung des Datenvermittlungsdienstes erhoben werden (wie etwa Datum, Uhrzeit und Geolokalisierungsdaten, Dauer der Tätigkeit sowie Verbindungen zu anderen natürlichen oder juristischen Personen) nur für die Entwicklung dieses Datenvermittlungsdienstes verwenden.</p> <p>Der Anbieter des Datenvermittlungsdienstes muss diese Daten den Dateninhabern auf Anfrage zur Verfügung stellen.</p>
Intention	Der Gesetzgeber möchte, dass die Anbieter von Datenvermittlungsdiensten die von den Dateninhabern bereitgestellten Daten zur Verbesserung ihrer Datenvermittlungsdienste verwenden können.
Rechtsgrundlagen	Art. 12 lit. c DGA
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Interoperabilität zwischen Dateninhabern/betroffenen Personen
Beschreibung	<p>Der Anbieter des Datenvermittlungsdienstes muss den Austausch der Daten in dem Format ermöglichen, in dem er diese von einer betroffenen Person oder vom Dateninhaber erhält.</p> <p>Der Anbieter des Datenvermittlungsdienstes darf die Daten nur in bestimmte Formate umwandeln, wenn mindestens eins der folgende Bedingungen erfüllt wird:</p> <p>(1) Wenn dies erforderlich ist um die Interoperabilität innerhalb und zwischen Sektoren zu verbessern.</p> <p>(2) Wenn der Datennutzer dies verlangt,</p>

	<p>(3) Wenn das Unionsrecht dies vorschreibt.</p> <p>(4) Wenn dies der Harmonisierung mit internationalen oder europäischen Datennormen dient.</p> <p>Der Anbieter des Datenvermittlungsdienstes muss es betroffenen Personen und Dateninhaber ermöglichen, auf die Umwandlung mittels Opt-out zu verzichten.</p>
Intention	Der Gesetzgeber möchte, damit der Binnenmarkt reibungslos funktionieren kann, dass Anbieter von Datenvermittlungsdiensten angemessene Maßnahmen ergreifen, um die Interoperabilität innerhalb eines Sektors und zwischen verschiedenen Sektoren sicherzustellen.
Rechtsgrundlagen	Art. 12 lit. d DGA
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

Name	Einrichtung von weiteren Diensten und Werkzeugen für betroffene Personen und Dateninhaber
Beschreibung	Wenn weitere Dienste und Werkzeuge zur Unterstützung von Dateninhabern und betroffenen Personen eingerichtet sind, bspw. um den Datenaustausch zu ermöglichen, muss der Anbieter des Datenvermittlungsdienstes sicherstellen, dass er diese nur auf expliziten Wunsch des Dateninhabers bzw. betroffenen Person zur Verfügung stellt.
Intention	Der Gesetzgeber möchte, dass Datenvermittlungsdienste Dateninhabern oder betroffenen Personen insbesondere zur Erleichterung des Datenaustauschs weitere Werkzeuge, z. B. durch vorübergehende Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung anbieten dürfen. Diese Werkzeuge und Dienste sollten nur auf ausdrücklichen Antrag oder mit der Zustimmung des Dateninhabers oder der betroffenen Person verwendet werden; und in diesem Zusammenhang angebotene Werkzeuge Dritter sollten Daten zu keinen anderen Zwecken verwenden.
Rechtsgrundlagen	Art. 12 lit. e DGA
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Einhaltung von Werten
Beschreibung	Der Anbieter des Datenvermittlungsdienstes muss sicherstellen, dass der Zugang sowohl für Betroffene als auch für Datennutzer und Dateninhaber fair, nichtdiskriminierend und transparent ist.
Intention	Der Gesetzgeber möchte, dass der Datenvermittlungsdienst grundlegende Werte einhält.
Rechtsgrundlagen	Art. 12 lit. f DGA
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

Name	Verfahren zur Verhinderung betrügerischer oder missbräuchlicher Praktiken
Beschreibung	Der Anbieter des Datenvermittlungsdienstes muss über ein Verfahren zur Verhinderung betrügerischer oder missbräuchlicher Praktiken bezogen auf die Parteien, die Zugang zum Datenvermittlungsdienst ersuchen, verfügen.
Intention	Der Gesetzgeber möchte, dass der Anbieter eines Datenvermittlungsdienstes über Verfahren zur Verhinderung betrügerischer oder missbräuchlicher Praktiken verfügt.
Rechtsgrundlagen	Art. 12 lit. g DGA
Impact auf das Projekt	Organisatorische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

Name	Gewährleistung von Interoperabilität zu anderen Diensten im selben Sektor
Beschreibung	Der Anbieter des Datenvermittlungsdienstes muss die Interoperabilität mit anderen Diensten, die im selben Sektor tätig sind durch die Nutzung von üblicherweise verwendeten offenen Standards gewährleisten.
Intention	Der Gesetzgeber möchte, damit der Binnenmarkt reibungslos funktionieren kann, dass Anbieter von Datenvermittlungsdiensten angemessene Maßnahmen ergreifen, um die Interoperabilität innerhalb eines Sektors und zwischen verschiedenen Sektoren sicherzustellen.
Rechtsgrundlagen	Art. 12 lit. i DGA

Impact auf das Projekt	Technische Randbedingung außerhalb des Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein

Name	Maßnahmen im Falle der Insolvenz
Beschreibung	Wenn der Anbieter eines Datenvermittlungsdienstes insolvent ist, muss dieser eine angemessene Weiterführung des Dienstes gewährleisten und Mechanismen einrichten, die es Dateninhabern und Datennutzern ermöglichen, Zugang zu ihren Daten zu erhalten, diese zu übertragen oder abzurufen und wenn Datenvermittlungsdiensten zwischen betroffenen Personen und Datennutzern erbracht werden, ihre Rechte auszuüben.
Intention	Der Gesetzgeber möchte, dass der Datenvermittlungsdienst auch im Falle der Insolvenz noch den Zugang zu Daten für Dateninhaber und Datennutzern ermöglicht.
Rechtsgrundlagen	Art. 12 lit. h DGA
Impact auf das Projekt	Out of Scope
Erfordert eine Nutzerinteraktion	nein

Name	Sicherheit von nicht personenbezogenen Daten
Beschreibung	Der Anbieter des Datenvermittlungsdienstes muss die Sicherheit von nicht personenbezogenen Daten gewährleisten, indem er Maßnahmen ergreift, um die rechtswidrige Übertragung und den rechtswidrigen Zugang zu diesen Daten zu verhindern. Personenbezogene Daten werden in der Vorschrift nicht explizit erwähnt, weil sich die entsprechende Anforderung bereits aus der DSGVO ergibt.
Intention	Der Gesetzgeber möchte, dass der Datenvermittlungsdienst auch die technische Sicherheit von nicht personenbezogenen Daten gewährleistet.
Rechtsgrundlagen	Art. 12 lit. j DGA
Impact auf das Projekt	Out of Scope
Erfordert eine Nutzerinteraktion	nein

Name	Meldung des unbefugten Umgangs mit Daten
Beschreibung	<p>Der Anbieter eines Datenvermittlungsdienstes muss die unbefugte Übertragung, den unbefugten Zugriff und die unbefugte Nutzung von nicht-personenbezogenen Daten dem Dateninhaber melden.</p> <p>Personenbezogene Daten werden in der Vorschrift nicht explizit erwähnt, weil sich die entsprechende Anforderung bereits aus der DSGVO ergibt.</p>
Intention	Der Gesetzgeber möchte, dass der Datenvermittlungsdienst transparent auch Informationen zu Vorfällen mit nicht personenbezogenen Daten bereitstellt.
Rechtsgrundlagen	Art. 12 lit. k DGA
Impact auf das Projekt	Out of Scope
Erfordert eine Nutzerinteraktion	ja

Name	Sicherheit von nicht personenbezogenen Daten bei der Speicherung, Verarbeitung und Übermittlung
Beschreibung	<p>Der Anbieter eines Datenvermittlungsdienstes muss die Sicherheit nicht personenbezogener Daten gewährleisten, indem er die notwendigen Maßnahmen ergreift, um ein angemessenes Sicherheitsniveau bei der Speicherung/Verarbeitung und Übermittlung sicherzustellen. Der Anbieter des Datenvermittlungsdienstes muss das höchste Sicherheitsniveau für die Übertragung wettbewerbsrelevanter Informationen sicherstellen.</p> <p>Personenbezogene Daten werden in der Vorschrift nicht explizit erwähnt, weil sich die entsprechende Anforderung bereits aus der DSGVO ergibt.</p>
Intention	Der Gesetzgeber möchte, dass der Datenvermittlungsdienst auch die technische Sicherheit von nicht personenbezogenen Daten gewährleistet und hierzu geeignete Maßnahmen ergreift.
Rechtsgrundlagen	Art. 12 lit. I DGA
Impact auf das Projekt	Out of Scope
Erfordert eine Nutzerinteraktion	nein

Name	Aufklärung betroffener Personen bei der Einholung von Einwilligungen
------	--

Beschreibung	<p>Der Anbieter des Datenvermittlungsdienstes muss betroffene Personen, bevor sie ihre Einwilligung erteilen, in prägnanter, transparenter, verständlicher und leicht zugänglicher Weise über die beabsichtigte Nutzung der Daten durch Datennutzer und die üblichen Geschäftsbedingungen für solche Nutzungen informieren und beraten.</p> <p>Der Anbieter des Datenvermittlungsdienstes muss die Rechteaübung der betroffenen Personen durch diese Maßnahmen erleichtern.</p>
Intention	Der Gesetzgeber möchte, dass der Datenvermittlungsdienst betroffene Personen hinreichend aufklärt, wenn Einwilligungen eingeholt werden. Ferner möchte der Gesetzgeber, dass der Datenvermittlungsdienst betroffene Personen bei der Geltendmachung von Betroffenenrechten unterstützt.
Rechtsgrundlagen	Art. 12 lit. m DGA
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	ja

Name	Zurverfügungstellen von Werkzeugen zur Einholung und zum Widerruf von Einwilligungen
Beschreibung	<p>Wenn Werkzeuge zur Einholung von Einwilligungen von betroffenen Personen bzw. von Erlaubnissen der Verarbeitung der vom Dateninhaber zur Verfügung gestellten Daten bereitgestellt werden, muss der Anbieter des Datenvermittlungsdienstes:</p> <p>(1) das Hoheitsgebiet des Drittlandes angeben, in dem die Datennutzung stattfinden soll;</p> <p>(2) den betroffenen Personen Werkzeuge zur Erteilung und zum Widerruf der Einwilligung zur Verfügung stellen;</p> <p>(3) Dateninhabern Werkzeuge zur Erteilung und zum Widerruf der Erlaubnis zur Verarbeitung von Daten zur Verfügung stellen.</p>
Intention	Der Gesetzgeber möchte, dass der Datenvermittlungsdienst betroffene Personen hinreichend aufklärt, wenn Werkzeuge zur Einholung von Einwilligungen von betroffenen Personen bzw. von Erlaubnissen der Verarbeitung der vom Dateninhaber zur Verfügung gestellten Daten bereitgestellt werden.
Rechtsgrundlagen	Art. 12 lit. n DGA
Impact auf das Projekt	Kernbestandteil eines Datenschutz-Cockpits

Erfordert eine Nutzerinteraktion	ja
---	----

Name	Führung eines Protokolls
Beschreibung	Der Anbieter des Datenvermittlungsdienstes muss Protokoll über seine Tätigkeit führen.
Intention	Der Gesetzgeber möchte, dass der Datenvermittlungsdienst einen Nachweis über seine Tätigkeiten führt.
Rechtsgrundlagen	Art. 12 lit. o DGA
Impact auf das Projekt	Optionaler Bestandteil eines Datenschutz-Cockpits
Erfordert eine Nutzerinteraktion	nein