



Der Minister

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie  
des Landes Nordrhein-Westfalen, 40190 Düsseldorf

An den Präsidenten  
des Landtags Nordrhein-Westfalen  
Herrn André Kuper MdL  
Platz des Landtags 1  
40221 Düsseldorf

LANDTAG  
NORDRHEIN-WESTFALEN  
17. WAHLPERIODE

**VORLAGE**  
**17/5842**

Alle Abg

15. Oktober 2021

Seite 1 von 2

## **Verwaltungsvereinbarung über die Weiterentwicklung und den Betrieb von FINK (Föderiertes Identitätsmanagement Interoperabler Nutzerkonten)**

Zuleitung nach Maßgabe der Parlamentsinformationsvereinbarung

Anlage: Entwurf der Verwaltungsvereinbarung über die Weiterentwicklung und den Betrieb von FINK (Föderiertes Identitätsmanagement Interoperabler Nutzerkonten) inkl. Anlagen

Sehr geehrter Herr Landtagspräsident,

gemäß Abschnitt II. Ziffern 1 und 3 der „Vereinbarung über die Unterrichtung des Landtags durch die Landesregierung“ übersende ich anbei den Entwurf der Verwaltungsvereinbarung über die Weiterentwicklung und den Betrieb von FINK (Föderiertes Identitätsmanagement Interoperabler Nutzerkonten).

Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG) verpflichtet den Bund und die Länder, Nutzerkonten bereitzustellen, über die sich Nutzerinnen und Nutzer bei der Inanspruchnahme von elektronischen Verwaltungsleistungen einheitlich identifizieren und authentifizieren können. Mit seiner Entscheidung 2019/43 hat der IT-Planungsrat zudem beschlossen, diese Nutzerkonten interoperabel zu gestalten. Damit soll ermöglicht werden, dass Nutzerinnen und Nutzer nach Registrierung bei dem Nutzerkonto eines Landes

Dienstgebäude und Lieferanschrift:  
Berger Allee 25  
40213 Düsseldorf

Telefon 0211 61772-0  
Telefax 0211 61772-777  
poststelle@mwide.nrw.de  
www.wirtschaft.nrw

Öffentliche Verkehrsmittel:  
Straßenbahnlinien 706, 708,  
709 bis Haltestelle Poststraße

auch Verwaltungsangebote der anderen Länder und des Bundes in Anspruch nehmen können. Das Nutzerkonto für natürliche Personen im Sinne des OZG für Nordrhein-Westfalen ist Servicekonto.NRW, dessen Zuständigkeit bei dem für Digitalisierung zuständigen Ministerium liegt.

Die vorliegende Verwaltungsvereinbarung operationalisiert die Entscheidung zur Interoperabilität der Nutzerkonten durch Etablierung einer „Föderation interoperabler Nutzerkonten“ (FINK) des Bundes und der Länder. Die Vereinbarung regelt insbesondere die Rahmenbedingungen für die weitere Ausgestaltung und Entwicklung der Föderation sowie deren organisatorische Umsetzung.

Die Umsetzungskosten der Verwaltungsvereinbarung trägt der IT-Planungsrat. Es ergeben sich keine Belastungen öffentlicher Haushalte.

Die Landesregierung hat der vorgenannten Verwaltungsvereinbarung mit Beschluss vom 5. Oktober 2021 zugestimmt. Ich bitte um Weiterleitung an die Damen und Herren Abgeordneten.

Mit freundlichen Grüßen

A handwritten signature in blue ink, appearing to read 'Andreas Pinkwart', with a large, stylized flourish above the name.

Prof. Dr. Andreas Pinkwart



# Verwaltungsvereinbarung

über die

## Weiterentwicklung und den Betrieb von FINK (Föderiertes Identitätsmanagement Interoperabler Nutzerkonten)



Bund und Länder schließen folgende Vereinbarung:



# Inhalt

Präambel	3
Vereinbarungspartner	5
Zweck der Vereinbarung	5
Gegenstand der Vereinbarung	5
Federführung	6
KIOSK	6
Aufgaben des Produktteams FINK	7
Beschlüsse des Produktteams FINK	8
Datenschutz und IT-Sicherheit	9
Haftung	10
Salvatorische Klausel	10
Inkrafttreten und Geltungsdauer der Vereinbarung	10

# Präambel

Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) vom 14.08.2017 sieht in § 3 Absatz 2 vor, dass Bund und Länder im Portalverbund Nutzerkonten bereitstellen, über die sich Nutzer für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren können.

Bereits zwei Jahre zuvor hatte sich der IT-Planungsrat grundsätzlich für eine flächendeckende Verbreitung von Servicekonten (die Begrifflichkeit Servicekonten ist analog dem Begriff Nutzerkonten im OZG zu verstehen) für Bürgerinnen, Bürger und Unternehmen ausgesprochen (Entscheidung 2015/17 vom 17.06.2015). In der Folge wurde die Interoperabilität der Nutzerkonten als Lösung zur Herstellung der flächendeckenden Verbreitung innerhalb der Projektgruppe eID-Strategie (PG eID-Strategie) herausgearbeitet und mit dem IT-Planungsrat zur weiteren Konzeption und Umsetzung abgestimmt.

Mit der Entscheidung 2018/41 des IT-Planungsrates vom 25.10.2018 zur eID-Strategie konnte die Umsetzung der Interoperabilität der Nutzerkonten gemäß der bisherigen Planung der PG eID-Strategie fortgeführt und die stufenweise Umsetzung begonnen werden. In einem ersten Schritt erfolgte die Herstellung der Interoperabilität der Nutzerkonten für Bürger, die in der Folge pilotiert und im Anschluss flächendeckend in Deutschland bereitgestellt werden soll.

Mit der Entscheidung 2019/43 des IT-Planungsrates in seiner 30. Sitzung vom 29.10.2019 bittet der IT-Planungsrat die PG eID-Strategie, ihre Arbeiten zur Umsetzung der Interoperablen Servicekonten bis zum 31. Dezember 2022 fortzusetzen.

In einem weiteren Schritt wird die Interoperabilität von Postfächern gemäß IT-PLR Entscheid 2020/04 vom 25. März 2020 zum Rollout von Postfächern umgesetzt. Auch die Interoperabilität von Organisationskonten im Kontext von ELSTER und eine Interoperabilität in erweiterten Kontexten wie der Justiz und für weitere Basisdienste sind wichtige Aufgaben.

Daher wird angestrebt, dass der IT-Planungsrat das Projekt „Interoperable Servicekonten“ spätestens ab dem Jahr 2022 zum Produkt des IT-Planungsrats erklärt. Der Freistaat Bayern wurde durch die PG eID-Strategie beauftragt, die Interoperabilität federführend umzusetzen.

Aus Gründen des Investitionsschutzes, aber auch des föderalen Wettbewerbs mit der Stärkung der Innovationskraft und dem Prinzip des Teilens von erfolgreichen Lösungen, haben Bund und Länder vereinbart, eine Föderation „Interoperable Servicekonten“ aufzubauen. Die Föderation für Interoperable Servicekonten stellt in diesem Zusammenhang durch Schaffung einer Identitätsföderation zukünftig sicher, dass Bürgerinnen und Bürger mit ihrem jeweiligen Nutzerkonto ihres Bundeslandes oder des Bundes deutschlandweit Verwaltungsleistungen auch anderer Verwaltungsportale von Bund und Ländern sicher und nutzerfreundlich in Anspruch nehmen können. Damit spielt die Identitätsföderation eine entscheidende Rolle für den Erfolg der Digitalisierung der öffentlichen Verwaltung in Deutschland. Für das Gelingen dieses föderalen Vorhabens hat der Freistaat Bayern das Kompetenzzentrum Interoperable Servicekonten (KIOSK) als Föderationsverwaltung bereitgestellt. KIOSK ist dabei die Organisationseinheit, die entsprechend der Beauftragung des Bayerischen Staatsministeriums für Digitales in Bayern die technischen Voraussetzungen und die organisatorischen Rahmenbedingungen der Interoperabilität der Nutzerkonten in Deutschland herstellt. Die Organisationseinheit KIOSK führt die Erstellung, Wartung und Pflege der Schnittstellen für die Interoperabilität, für den Meta-

datenservice, für die gegenseitige Vertrauensstellung der Nutzerkonten und die Regeln für eine erfolgreiche Umsetzung der Interoperabilität durch. In diesem Rahmen wird das Produkt „FINK“ (Föderiertes Identitätsmanagement Interoperabler Nutzerkonten in Deutschland) von KIOSK erstellt. KIOSK ist organisatorisch zum Zeitpunkt des Abschlusses der Verwaltungsvereinbarung dem Bayerischen Staatsministerium der Finanzen und für Heimat, bzw. zukünftig dem im Rahmen der Geschäftsverteilung des Freistaates Bayern nachfolgenden Ministerium, zugeordnet.

Das Produkt FINK besteht aus dem Metadatenservice, den Spezifikationen von Schnittstellen und den Test- und Integrationsumgebungen (den sog. FINK.Labs). Zentral sind dabei die Schnittstellen der Interoperabilität von Nutzerkonten, Postfächern und weiterer Basisdienste. Alle notwendigen Informationen für die Vereinbarungspartner der Föderation werden auf einer eigens dafür seitens KIOSK bereitgestellten Informationsplattform abgelegt.

Diese Vereinbarung regelt die Rahmenbedingungen für die weitere Ausgestaltung und Entwicklung der Föderation FINK über das Produkt FINK sowie deren organisatorische Umsetzung im KIOSK für Bund und Länder. Bund und Länder treten mit Unterzeichnung der Beitrittserklärung in Anlage 1 bzw. Anlage 2 der Föderation FINK bei.

Der Aufbau der Föderation FINK zugrundeliegenden Identitätsföderation FINK, in der sich die Vereinbarungspartner auf Mindeststandards für Sicherheit einigen müssen, wird begleitet durch das BSI in Form einer Technischen Richtlinie. Das Dokument „TR-03160-2 Servicekonten Teil 2: Interoperables Identitätsmanagement für Bürgerkonten“ erläutert den Aufbau der Interoperablen Nutzerkonten und stellt eine Richtschnur für die IT-Sicherheits-Anforderungen an die Vereinbarungspartner dieser Identitätsföderation dar.

Die Nutzerkonten der Länder und des Bundes mit ihren Basisdiensten setzen die im OZG geforderten Nutzerkonten um und verbleiben Verfahren der Länder bzw. des Bundes. Die Föderation FINK mit ihrer Identitätsföderation schafft durch den Metadatenserver, den Regelungen und Spezifikationen von Schnittstellen die Voraussetzungen, dass die aus dem OZG abzuleitenden Vorgaben zur Interoperabilität von Nutzerkonten mit dieser Vereinbarung erfüllt werden können.

Soweit in dieser Vereinbarung das Bayerische Staatsministerium für Digitales (StMD) aufgeführt ist, tritt an dessen Stelle bei einer organisatorischen Änderung das im Rahmen des Geschäftsverteilungsplanes des Freistaates Bayern nachfolgende Ministerium.

## §1

# Vereinbarungspartner

Vereinbarungspartner können

- a) der Bund und
- b) die Länder

sein.

Der Beitritt zur Vereinbarung erfolgt gemäß Beitrittserklärung (s. Anlage 1 bzw. Anlage 2 zu dieser Vereinbarung).

## §2

# Zweck der Vereinbarung

Diese Verwaltungsvereinbarung dient ausgehend vom OZG der kooperativen Herstellung der Interoperabilität der Nutzerkonten von Bund und Ländern.

## §3

# Gegenstand der Vereinbarung

- (1) Die kooperative Herstellung der Interoperabilität nach § 2 umfasst die Planung und Entwicklung sowie den Betrieb, die Wartung und die Pflege der erforderlichen technischen Spezifikationen und Komponenten, ebenso die Weiterentwicklung der zugrundeliegenden Prozesse sowie die Erarbeitung neuer Prozesse.

Das Produkt FINK besteht aus dem Metadatenservice, den Spezifikationen von Schnittstellen und den Test- und Integrationsumgebungen (den sog. FINK.Labs). Zentral sind dabei die Schnittstellen der Interoperabilität:

- von Nutzerkonten für Bürger und Organisationen,
- von Postfächern
- und weiteren Basisdiensten (z.B. Statusmeldungen), die im Rahmen der Weiterentwicklung umgesetzt werden.

Die technische Anbindung der Nutzerkonten verantworten die Vereinbarungspartner in eigener Zuständigkeit.

- (2) Die Vereinbarungspartner verantworten die Weiterentwicklung des Produktes FINK im Rahmen der in dieser Verwaltungsvereinbarung beschriebenen Regelungen.
- (3) Die Finanzierung der Planung, Entwicklung, Wartung, Pflege und des Betriebes des Produktes FINK erfolgt durch den IT-Planungsrat.

## § 4

# Federführung

Der Freistaat Bayern, vertreten durch das Bayerische Staatsministerium für Digitales,

1. stimmt die Verwaltungsvereinbarung mit Bund und Ländern ab
2. verantwortet die Mittelbewirtschaftung in enger Abstimmung mit der FITKO
3. beauftragt in Bayern das IT-DLZ mit der Einrichtung von KIOSK und den damit verbundenen Aufgaben
4. kann im Rahmen der durch den IT-Planungsrat bereitgestellten Mittel Dritte mit der Erbringung von Dienstleistungen zur Umsetzung der zentralen Komponenten (Metadaten-server und FINK.Labs) und der Informationsplattform beauftragen oder dem IT-DLZ die Befugnis zur Auftragserteilung übertragen.
5. berichtet dem IT-Planungsrat, der FITKO und der PG eID-Strategie regelmäßig über den Umsetzungsstand.

## § 5

# KIOSK

- (1) KIOSK ist die Organisationseinheit, die im Auftrag des Bay. Staatsministeriums für Digitales und nach dessen fachlichen Weisungen den technischen Betrieb der zentralen Komponenten und der Informationsplattform verantwortet sowie die Weiterentwicklung der zentralen Komponenten des Produktes FINK, ausgehend von den Beschlüssen des Produktteams FINK, gewährleistet.
- (2) Zur Unterstützung des Produktteams FINK richtet KIOSK eine Geschäftsstelle ein, die die operative Steuerung des Produktes FINK übernimmt. Die Geschäftsstelle setzt sich aus Vertretern des KIOSK zusammen.
- (3) Die Aufgaben der Geschäftsstelle FINK setzen sich insbesondere wie folgt zusammen:
  1. Organisation der Termine und der Agenda des Produktteams FINK
  2. Erster Kontakt für die Vereinbarungspartner für Fragen zum Produkt FINK und zum Produktteam FINK
  3. Koordination Wissensmanagement und Informationsaustausch
  4. Koordination der Abstimmungen zwischen den Beteiligten
  5. Koordination der Veröffentlichungen von Entscheidungen

6. Pflege und Weiterentwicklung der Informationsplattform KIOSK/FINK
7. Koordination der Umsetzung der Beschlüsse des Produktteams FINK und Steuerung des technischen Betriebs des Produktes FINK
8. Überprüfung/Unterstützung von neuen Vereinbarungspartnern der Föderation FINK anhand der Aufnahmebedingungen
9. Erstellung von Empfehlungen an das Produktteam FINK
10. Aufnahme und Bewertung von Anforderungen
11. Benachrichtigung der bestehenden Vereinbarungspartner über den Beitritt neuer Vereinbarungspartner

Weitere vergleichbare Aufgaben können durch das Produktteam FINK im Rahmen einer Geschäftsordnung für die Geschäftsstelle festgelegt werden. Die Geschäftsordnung kann nur durch einstimmigen Beschluss des Produktteams FINK erstellt und geändert werden.

## § 6

### Produktteam FINK

- (1) Für die kooperative Herstellung der Interoperabilität durch das Produkt FINK und deren Weiterentwicklung wird das Produktteam FINK eingerichtet, das sich aus je einer stimmberechtigten Vertreterin oder einem stimmberechtigten Vertreter der Vereinbarungspartner zusammensetzt. Den Vorsitz führt der Freistaat Bayern, vertreten durch das Bayerische Staatsministerium für Digitales.
- (2) Das Produktteam FINK tagt mindestens zweimal pro Jahr auf Einladung des Vorsitzes. Es richtet bei Bedarf Unterarbeitsgruppen ein und kann zur fachlichen Unterstützung seiner Aufgaben Dritte einbeziehen, die an den Sitzungen ohne Stimmberechtigung teilnehmen
- (3) Die Vereinbarungspartner tragen die ihnen aus der Tätigkeit des Produktteams und seiner Unterarbeitsgruppen jeweils entstehenden Kosten selbst.

## § 7

### Aufgaben des Produktteams FINK

Die Aufgaben des Produktteams FINK sind:

1. Gesamtsteuerung des Produktes FINK
2. Entscheidung über Haushalts- und Finanzplanung zur Finanzierung des Produktes FINK durch Mittel des IT-Planungsrates ausgehend von den Vorgaben der FITKO

3. Koordination der bedarfsgerechten strategischen und operativen Weiterentwicklung des Produktes FINK im Hinblick auf Interoperable Nutzerkonten und deren Basisdienste (hier Stand Dezember 2019):

- a) Authentifizierungskomponente für Bürger
- b) Postfach für Bürger
- c) Authentifizierungskomponente für juristische Personen (sog. Organisationskonten)
- d) Postfach für juristische Personen
- e) Festlegung gemeinsamer Mindestanforderungen der IT-Sicherheit und Maßnahmen zu deren Umsetzung.

Hierzu gehört auch die Priorisierung der Anforderungen.

4. Beauftragung der Geschäftsstelle FINK gemäß Beschluss des Produktteams FINK.

## § 8

### Beschlüsse des Produktteams FINK

(1) Das Produktteam FINK entscheidet mit einer Mehrheit von zwei Drittel der teilnehmenden Vereinbarungspartner, welche mindestens zwei Drittel der Finanzierungsanteile der Vereinbarungspartner am Produkt FINK abbildet.

Ein Mitglied des Produktteams FINK kann sein Stimmrecht für eine Sitzung oder Teile einer Sitzung auf einen anderen Vereinbarungspartner übertragen, wenn er selbst an der Teilnahme gehindert ist. Die Stimmrechtsübertragung muss mindestens in Textform erklärt und zu Protokoll genommen werden. Sie muss die konkrete Sitzung bzw. den Teil der Sitzung benennen, für den sie erfolgt. Einem Vereinbarungspartner kann maximal ein Stimmrecht übertragen werden.

(2) Stimmenthaltungen werden bei der Beschlussfassung nicht gezählt.

(3) Jeder Vereinbarungspartner der Vereinbarung ist berechtigt, im Einvernehmen mit KIOSK und den anderen Vereinbarungspartner auf eigene Rechnung zusätzliche Anforderungen an FINK zur Umsetzung an die Geschäftsstelle in Auftrag zu geben. Ein besonderes Nutzungsrecht wird durch die Umsetzung der zusätzlichen Anforderungen nicht erworben. Um inkonsistente Programmstände zu verhindern, werden die separaten Entwicklungen Bestandteil des Gesamtcodes und somit auch Bestandteil der Wartung und Pflege. In den Fällen des § 12 Abs. 3 entscheiden die verbleibenden Vertragspartner, ob die separaten Entwicklungen weiter Bestandteil der Wartung und Pflege sind oder aus dem Programmcode entfernt werden.

(4) Die Mitglieder des Produktteams FINK stimmen die Anforderungen an das Produkt FINK jeweils so ab, dass in den Sitzungen des Produktteams FINK für das jeweilige Land und den Bund verbindliche Voten abgegeben werden können.

(5) Die Geschäftsstelle setzt den Termin der nächsten Sitzung fest. Anträge zur Tagesordnung sollen mit allen Antragsunterlagen mindestens vier Wochen vor dem Termin der nächsten Sitzung bei der Geschäftsstelle eingereicht werden. In dringenden Fällen kann einvernehmlich auf die Einhaltung der Frist verzichtet werden.

- (6) Die Antragsunterlagen für die Tagesordnung müssen die fachlichen, strategischen, organisatorischen, personellen, wirtschaftlichen, technischen und sicherheitsrelevanten Informationen enthalten, die zur Entscheidungsfindung erforderlich sind. KIOSK erstellt auf Basis der eingereichten Unterlagen ein Grobkonzept sowie eine Aufwandsschätzung und stellt diese dem Produktteam FINK zur Verfügung. Die Geschäftsstelle kann jederzeit weitere Unterlagen und die Beantwortung entscheidungsrelevanter Fragen anfordern. Sie kann die Behandlung von Tagesordnungspunkten von deren fristgemäßer Vorlage abhängig machen.
- (7) Die Antragsunterlagen werden mit der Anmeldung zur Tagesordnung allen Vereinbarungspartnern durch die Geschäftsstelle zugeleitet.
- (8) Über die Sitzungen des Produktteams FINK ist ein Ergebnisprotokoll zu führen, dessen Entwurf mit den Vereinbarungspartnern abgestimmt und dessen endgültige Fassung von der Geschäftsstelle erstellt und an die Vereinbarungspartner versandt oder an zentraler Stelle zum Abruf bereitgestellt wird. Abweichende Voten werden im Protokoll festgehalten.
- (9) Beschlüsse können auch im Umlaufverfahren herbeigeführt werden. Der Vorsitzende veranlasst das Umlaufverfahren auf Antrag eines Vereinbarungspartners; § 8 Abs. 1 bis 8 finden entsprechende Anwendung. Ein Umlaufverfahren soll die Dauer von zwei Wochen nicht unterschreiten.

## § 9

### Datenschutz und IT-Sicherheit

- (1) Innerhalb der zentralen Komponenten (Metadatenserver und FINK.Labs) zur Herstellung der Interoperabilität werden nach dem derzeitigen Projektstand keine personenbezogenen Daten verarbeitet. Eine Weiterentwicklung der zentralen Komponenten, die eine Änderung im Hinblick auf die datenschutzrechtliche Relevanz zur Folge hätte, ist nur vorbehaltlich der Zustimmung des Freistaates Bayern möglich. Sollten die Vereinbarungspartner eine Weiterentwicklung beschließen, die zu einer Verarbeitung personenbezogener Daten im Rahmen dieser zentralen Komponenten führt, werden die Vereinbarungspartner die Vereinbarung über die datenschutzrechtliche Verantwortlichkeit neu regeln.
- (2) Die datenschutzrechtliche Verantwortung für die Verarbeitung der personenbezogenen Daten in den mit den zentralen Komponenten verknüpften Nutzerkonten richtet sich nach der Vereinbarung über gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 S. 1 Datenschutz-Grundverordnung (DSGVO) gemäß Anlage 3 zu dieser Vereinbarung.
- (3) In der Identitätsföderation müssen die Vereinbarungspartner der Föderation die Mindeststandards für Sicherheit festlegen, auf die sich alle Vereinbarungspartner einigen können. Die Mindeststandards berücksichtigen die Anforderungen der DSGVO für den Schutz der Rechte und Freiheiten der betroffenen Personen und die Details zu deren Überwachung durch die Föderationsverwaltung KIOSK.

## § 10

# Haftung

Aufgrund der gemeinschaftlichen Planung und Steuerung des Produktes FINK ist eine Haftung der betreibenden Vereinbarungspartner des Produktes FINK, insbesondere für technische und inhaltliche Fehler oder fehlende Verfügbarkeit, gegenüber den übrigen Vereinbarungspartnern ausgeschlossen, außer es handelt sich um vorsätzliches oder grob fahrlässiges Handeln oder bei Verletzungen von Leib, Leben und Gesundheit.

## § 11

# Salvatorische Klausel

- (1) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Abschluss dieser Vereinbarung unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit der Vereinbarung im Übrigen unberührt.
- (2) Die Vereinbarungspartner verpflichten sich, anstelle dieser unwirksamen Bestimmungen auf die Beschlussfassung und Aufnahme derjenigen wirksamen Bestimmungen in dieser Vereinbarung hinzuwirken, welche dem Sinn und Zweck der unwirksamen Bestimmungen am meisten entsprechen.

## § 12

# Inkrafttreten und Geltungsdauer der Vereinbarung

- (1) Diese Vereinbarung tritt für die Gremien und die Organisationseinheit KIOSK zum \_01.11.2020\_ in Kraft.
- (2) Mit der Unterzeichnung der Beitrittserklärung gemäß Anlage 1 bzw. 2 wird die Vereinbarung für den beitretenden Vereinbarungspartner wirksam.
- (3) Diese Vereinbarung kann von jedem Vereinbarungspartner unter Einhaltung einer sechsmo-natigen Frist zum Jahresende gekündigt werden.
- (4) Die Kündigung ist dem Vorsitz und der Geschäftsstelle FINK schriftlich zu erklären. Sie wirkt gegenüber allen Vereinbarungspartnern. Mit der Kündigung scheidet der Vereinbarungspart-ner aus und die Vereinbarung besteht mit den anderen Vereinbarungspartnern fort. Die Kom-ponenten des ausscheidenden Vereinbarungspartners werden mit dem Wirksamwerden sei-ner Kündigung nicht mehr von der Föderation FINK bedient. Nähere Details können in der Geschäftsordnung geregelt werden.
- (5) Die Vereinbarung tritt auf einstimmigen Beschluss der Vereinbarungspartner außer Kraft. In dem Beschluss sind der Zeitpunkt und die finanziellen Auswirkungen des Außerkrafttretens zu regeln.

## Anlagen:

Anlage 1: Beitrittserklärung

Anlage 2: Absichtserklärung über den Beitritt (Beitrittserklärung unter Vorbehalt)

Anlage 3: Vereinbarung über gemeinsame Verantwortlichkeit  
nach Art. 26 Abs. 1 S. 1 Datenschutz-Grundverordnung (DSGVO)



## Beitrittserklärung zur Verwaltungsvereinbarung über die Weiterentwicklung und den Betrieb von FINK (als Vereinbarungspartner)

Hiermit erkläre ich für das Land/den Bund \_\_\_\_\_ den Beitritt zum Föderierten Identitätsmanagement Interoperabler Nutzerkonten (FINK) gemäß der Verwaltungsvereinbarung.

Der Beitritt erfolgt mit Wirkung zum \_\_\_\_\_.

Der Beitretende führt das Nutzerkonto \_\_\_\_\_ (*bitte die URL benennen*), nach dem sich sein Wirkbereich im Rahmen der gemeinsamen Verantwortlichkeit im Sinne des Art. 26 DSGVO gemäß der als Anlage 3 zur Verwaltungsvereinbarung beigefügten Vereinbarung richtet.

Es wird versichert, dass der Beitretende die gesetzlichen und vertraglichen Grundlagen der Zusammenarbeit, insbesondere die datenschutzrechtlichen Rahmenbedingungen geprüft hat und ihre Umsetzung in seinem Land/dem Bund gewährleisten wird.

\_\_\_\_\_  
(Unterschrift)

\_\_\_\_\_  
(Ort, Datum)



# Vereinbarung über die gemeinsame Verantwortlichkeit nach Art. 26 Datenschutz-Grundverordnung (DSGVO)

## Präambel

Diese Vereinbarung ist als Anlage 3 ein Bestandteil der Verwaltungsvereinbarung über die Weiterentwicklung und den Betrieb von FINK (im Folgenden: Verwaltungsvereinbarung). Die Vereinbarungspartner übernehmen mit ihrem Beitritt zur Verwaltungsvereinbarung Rechte und Pflichten aus dieser Vereinbarung. Mit der Angabe ihres Nutzerkontos in der Beitrittserklärung (Anlage 1 bzw. Anlage 2) definieren sie ihre Verantwortlichkeit im Sinne des § 2.

Das gemäß der Verwaltungsvereinbarung gemeinsam betriebene Produkt FINK im Projekt „Interoperable Servicekonten“ erlaubt, die bei einem der Vereinbarungspartner angelegten Nutzerkonten, Postfächer und weiteren Basisdienste für die Verwaltungsfachverfahren der anderen Vereinbarungspartner zu nutzen, indem es eine interoperable Kommunikation zwischen den genannten IT-Komponenten herstellt. In diesem Zusammenhang bestimmen die Vereinbarungspartner über das Mittel der Verarbeitung von personenbezogenen Daten innerhalb der Interoperablen Nutzerkonten gemeinsam. Ihr Wirken als gemeinsam Verantwortliche im Sinne des Art. 26 DSGVO richtet sich nach dieser Vereinbarung.

## Hintergrund: Darstellung der technischen Umsetzung zur Nachvollziehbarkeit der Verarbeitung personenbezogener Daten

Innerhalb der Nutzung der interoperablen Nutzerkonten werden folgende Vorgänge im Hinblick auf die datenschutzrechtliche Relevanz betrachtet:

- Anmeldung mittels Interoperabler Nutzerkonten
- Interoperabilität der Postfächer

Die vom Freistaat Bayern betriebene Informationsplattform, für die sich die Mitarbeiter der Vereinbarungspartner der Föderation FINK anmelden, verarbeitet die Daten der registrierten Nutzer (Mitarbeiter der Vereinbarungspartner der Föderation FINK) in eigener Verantwortung. Sie ist nicht Gegenstand dieser Vereinbarung über die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO.

### 1. Anmeldung mittels Interoperabler Nutzerkonten:

Im Kontext der Interoperabilität von Nutzerkonten sind folgende IT-Komponenten beteiligt und kommunizieren über die in der Abbildung 1 gezeigten nachfolgend dargestellten Wege.

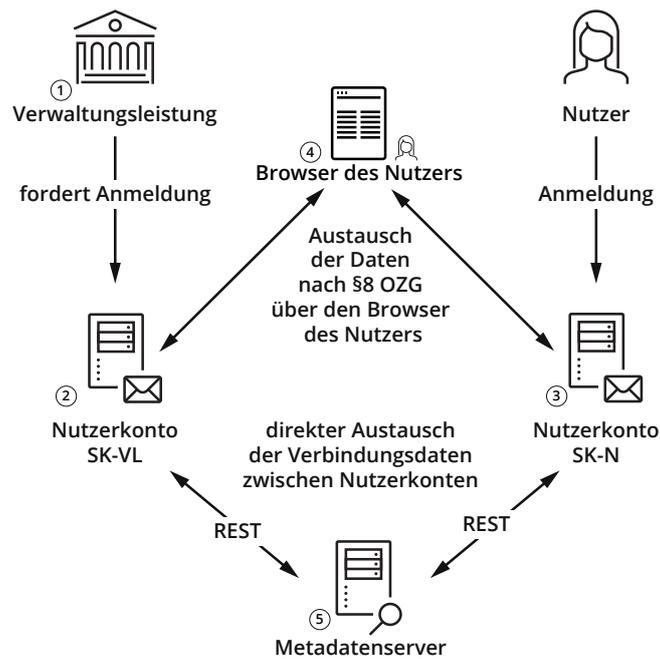


Abbildung 1: Überblick über die Kommunikationswege

Zu betrachtende IT-Komponenten:

- 1) Die Verwaltungsleistung
- 2) Das Nutzerkonto, an das die Verwaltungsleistung angebunden ist (SK-VL)
- 3) Das Nutzerkonto des Nutzers (SK-N)
- 4) Die technischen IT-Komponenten des Nutzers, also sein Endgerät (z.B. PC) mit Browser
- 5) Der Metadatenserver

Die Anmeldung (Login) eines Nutzers findet am Nutzerkonto SK-N statt. Das Nutzerkonto SK-N überträgt die gemäß § 8 OZG in der jeweils geltenden Fassung (oder gemäß der Nachfolgevorschrift) bestimmten Daten des Nutzers signiert und verschlüsselt an das Nutzerkonto SK-VL. **Die Anmeldung des Nutzers am Nutzerkonto SK-N ist aus datenschutzrechtlicher Sicht relevant.**

Damit das Nutzerkonto SK-N die Daten an das Nutzerkonto SK-VL und somit indirekt an die Verwaltungsleistung weitergeben kann, müssen sich die Nutzerkonten gegenseitig finden und vertrauen können. Anschließend kann eine Weiterleitung des Nutzers an das korrekte Nutzerkonto durchgeführt werden. Dazu befragen die Nutzerkonten regelmäßig den Metadatenserver nach der veröffentlichten Adressliste plus Metadaten der Nutzerkonten in der Föderation FINK. Die Metadaten enthalten ausschließlich technische Informationen zur eindeutigen Adressierung des Nutzerkontos (z.B. der BayernID), die öffentlichen Schlüssel der verwendeten X509-Zertifikate, die unterstützten HTTP-Anfrage-Methoden (GET, POST), die eingesetzten Verschlüsselungs-, Signatur- und Hash-Verfahren sowie weitere technische Informationen, um eine sichere Verbindung zwischen Nutzerkonten herzustellen.

## (1) Nutzerkonten und Basisdienste

Für die datenschutzrechtliche Betrachtung der IT-Komponenten erfolgt die Darstellung der Datenflüsse sowie der Datenverarbeitung personenbezogener Daten auf Basis von Anwendungsfällen.

### Anwendungsfall 1:

Anmeldung des Nutzers an einer Verwaltungsleistung bei Nutzung der Interoperabilität

Im Kontext der Anmeldung an einer Verwaltungsleistung im interoperablen Fall sind die IT-Komponenten der Verwaltungsleistung selbst (①), des Nutzerkontos, an das die Verwaltungsleistung angeschlossen ist (② SK-VL), und des Nutzerkontos des Nutzers (③ SK-N) an einer Datenverarbeitung von personenbezogenen Daten beteiligt. Allerdings ist die Verwaltungsleistung an sich kein Gegenstand des Projekts zur Herstellung der Interoperabilität der Nutzerkontosysteme.

Der Metadatenserver (④) ist in diesem Anwendungsfall keine beteiligte IT-Komponente, da er im Kontext dieses Anwendungsfalls nicht an einer Kommunikation teilnimmt, also zu keinem Zeitpunkt personenbezogene Daten des Nutzers erhält oder verarbeitet.

Der Browser des Nutzers (⑤) wird in der Abbildung 1 ausschließlich aus Gründen der Vollständigkeit aufgeführt. Der Browser ist eine IT-Komponente des Nutzers und nicht eines Vereinbarungspartners. Für die Übertragung und Anzeige der personenbezogenen Daten des Nutzers stellt der Browser jedoch einen integralen Bestandteil der Kommunikation dar.

### Ergebnis:

Die Verarbeitung der Daten gemäß § 8 OZG in der jeweils geltenden Fassung (oder gemäß der Nachfolgevorschrift) am Nutzerkonto (② SK-VL), an das die Verwaltungsleistung angeschlossen ist, und am Nutzerkonto des Nutzers (③ SK-N) sind aus datenschutzrechtlicher Sicht relevant.

### Anwendungsfall 2:

Anmeldung des Nutzers an einem Basisdienst bei Nutzung der Interoperabilität

Dieser Anwendungsfall stellt einen Spezialfall des Anwendungsfalls 1 dar. An die Stelle der Verwaltungsleistung tritt das Nutzerkonto (② SK-VL) oder ein mit dem Nutzerkonto verbundener Basisdienst. Der Basisdienst ist im selben Wirkungsbereich wie das Nutzerkonto. Beispiele für Basisdienste sind ein Bescheidabholdienst, ein Datenschutzcockpit oder ein Postfach.

Im Kontext der Anmeldung an einem Basisdienst im interoperablen Fall sind die IT-Komponenten des Basisdienstes, der zum Nutzerkonto der Verwaltungsleistung (② SK-VL) gehört, des Nutzerkontos (② SK-VL) selbst und des Nutzerkontos des Nutzers (③ SK-N) an einer Datenverarbeitung von personenbezogenen Daten beteiligt.

Der Metadatenserver (④) ist in diesem Anwendungsfall keine beteiligte IT-Komponente, da er im Kontext dieses Anwendungsfalls nicht an einer Kommunikation teilnimmt, also zu keinem Zeitpunkt personenbezogene Daten des Nutzers erhält oder verarbeitet.

Der Browser des Nutzers wird in der Abbildung 1 ausschließlich aus Gründen der Vollständigkeit aufgeführt. Der Browser ist eine IT-Komponente des Nutzers und nicht eines Vereinbarungspartners. Für die Übertragung und Anzeige der personenbezogenen Daten des Nutzers stellt der Browser jedoch einen integralen Bestandteil der Kommunikation dar.

**Ergebnis:**

Die Verarbeitung der Daten gemäß § 8 OZG in der jeweils geltenden Fassung (oder gemäß der Nachfolgevorschrift) an dem Basisdienst, am Nutzerkonto, an das der Basisdienst angeschlossen ist, und am Nutzerkonto des Nutzers sind aus datenschutzrechtlicher Sicht relevant.

Hinweis: Anwendungsfälle, die Interaktionen und Datenverarbeitungsvorgänge personenbezogener Daten der Nutzer außerhalb der Nutzung der Interoperabilität der Nutzerkonten beinhalten, sind nicht Gegenstand der Betrachtung, da sie nicht Teil der Verwaltungsvereinbarung sind. Diese Anwendungsfälle werden nicht über die Interoperabilität abgewickelt und daher gesondert durch den für die beteiligten IT-Komponenten verantwortlichen Vereinbarungspartner selbst verantwortet. Hierunter fallen z.B. die Anwendungsfälle „Anmeldung zur Nutzung einer lokalen Verwaltungsleistung“ oder „Anmeldung zur Nutzung eines lokalen Basisdiensts (z.B. Passwort ändern oder persönliches Postfach einsehen)“.

**Ergebnis:** Eine datenschutzrechtliche Relevanz für die Verwaltungsvereinbarung besteht bei diesen Anwendungsfällen nicht, da keine Kommunikation zwischen den IT-Komponenten der Vereinbarungspartner erfolgt. Im Kontext dieser Anwendungsfälle sind die IT-Komponenten entkoppelt und unabhängig.

(2) Zentrale Komponenten

Es folgt die Betrachtung der Anwendungsfälle zur Herstellung der Vertrauensstellung zwischen den Nutzerkonten der Vereinbarungspartner.

Für die Herstellung einer Vertrauensstellung zwischen den Nutzerkonten sind ausschließlich die Nutzerkonten der Vereinbarungspartner (Ⓒ und Ⓓ) und des MetadatenServers (Ⓔ) beteiligt.

**Ergebnis:** Bei dieser technischen Kommunikation über eine Maschine-Maschine-Schnittstelle werden keine personenbezogenen Daten übertragen oder verarbeitet. Jedoch ist die Richtigkeit der Angaben zum Aufbau einer Vertrauensstellung eine unabdingbare Voraussetzung für eine dann datenschutzgerechte Kommunikation zwischen den Nutzerkonten. Die datenschutzrechtliche Betrachtung gemäß Art. 26 DSGVO zum Schutz der Rechte des Nutzers bei der Verarbeitung seiner personenbezogenen Daten beschränkt sich in diesem Fall auf die einschlägigen Maßnahmen zur Erfüllung der Anforderungen entsprechend aus Art. 32 DSGVO.

## 2. Interoperabilität der Postfächer

### (1) Postfächer

Die Teilnehmer am FINK-Postfachnetzwerk sind deutsche Behörden, die online Verwaltungsleistungen im Kontext des OZG anbieten, sowie die Bürger als Nutzer dieser Dienste. Die Behörden müssen die Möglichkeit haben, während der Ausführung der Verwaltungsleistung mit ihren Nutzern elektronisch Daten auszutauschen. Für diesen Datenaustausch wird der Postfachdienst eines Nutzerkontos genutzt.

Wenn der Nutzer einer Verwaltungsleistung über die Interoperabilität ein anderes Nutzerkonto als das nutzt, an welches die Verwaltungsleistung der Behörde angeschlossen ist, dann müssen die Nutzerkonten mit ihren Postfächern personenbezogene Daten wie z.B. die Postfachreferenz übermitteln und verarbeiten, um einen Nachrichtenversand zwischen Behörde und Nutzer zu ermöglichen. Im Vorfeld muss der Nutzer hierzu einen Zugang eröffnet und dem Empfang von Nachrichten einer Behörde zugestimmt haben. Technisch führt dieser Sachverhalt zu einer typischen eDelivery-Architektur mit vier Systemen („4-Corner-Modell“), bei der die IT-Komponenten des Nutzerkontos als ERDS-Anbieter (Electronic Registered Delivery Service) für die tatsächlichen Absender und Empfänger fungieren, wie in eIDAS beschrieben.

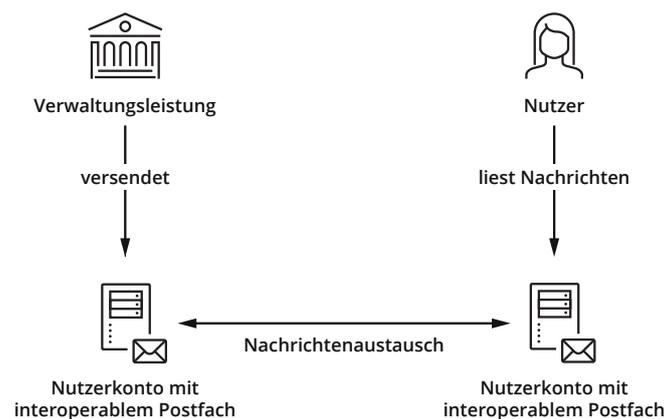


Abbildung 2: Überblick über die relevanten Teilnehmer

Die Kommunikation zwischen dem Postfach des Nutzerkontos SK-VL und dem Postfach des Nutzerkontos SK-N wird einheitlich und verbindlich über die Föderation FINK geregelt. Sie findet über eine direkte Verbindung und ausschließlich zwischen den Postfächern der beiden Nutzerkonten statt.

**Ergebnis:** Die Kommunikation zwischen den Postfächern ist aus datenschutzrechtlicher Sicht relevant.

### (2) Zentrale Komponenten

Zur Herstellung der Vertrauensstellung wird ebenfalls ein Metadatenserver verwendet. Der Metadatenserver speichert Konfigurationen für den Versand unterschiedlicher Nachrichtentypen. So wird beispielsweise die Anzahl erlaubter Anlagen oder die maximale Größe der Nachricht in Megabyte festgelegt. Ebenso werden Nachrichten anhand der Rechtsfolge unterschieden. Die

Metadaten zu diesen Nachrichtentypen enthalten weder einen Personenbezug noch einen Bezug zu einer konkreten Nachricht. Ferner enthalten die Metadaten ausschließlich technische Informationen zur eindeutigen Adressierung eines Postfachs (z.B. dem Postfach der BayernID), die öffentlichen Schlüssel der verwendeten X509-Zertifikate, die unterstützten Anfrage-Methoden, die eingesetzten Verschlüsselungs-, Signatur- und Hash-Verfahren sowie weitere technische Informationen, um einen sicheren Nachrichtenversand zwischen den Postfächern der Nutzerkonten herzustellen.

**Ergebnis:** Bei dieser technischen Kommunikation über eine Maschine-Maschine-Schnittstelle werden keine personenbezogenen Daten übertragen oder verarbeitet. Jedoch ist die Richtigkeit der Angaben zum Aufbau einer Vertrauensstellung eine unabdingbare Voraussetzung für eine dann datenschutzgerechte Kommunikation zwischen den Nutzerkonten mit ihren Postfächern. Die datenschutzrechtliche Betrachtung gemäß Art. 26 DSGVO zum Schutz der Rechte des Nutzers bei der Verarbeitung seiner personenbezogenen Daten beschränkt sich in diesem Fall auf die einschlägigen Maßnahmen zur Erfüllung der Anforderungen entsprechend Art. 32 DSGVO.

## § 1

Die Verarbeitung personenbezogener Daten erfolgt an den Nutzerkonten SK-VL und SK-N sowie den dazu gehörigen Postfächern. Jeder Vereinbarungspartner hat ein Nutzerkonto, mit dem er der Verwaltungsvereinbarung über die Weiterentwicklung und den Betrieb von FINK beiträgt. Die personenbezogenen Daten, die im Sinne dieser Vereinbarung erhoben werden, sind in § 8 OZG aufgezählt. Im Falle einer Gesetzesänderung, erfolgt eine Anpassung der Datenverarbeitung an den neuen Wortlaut des Gesetzes.

Für die Herstellung der Interoperabilität der Nutzerkonten (Zweck der Datenvereinbarung im Sinne dieser Vereinbarung) werden zentrale Komponenten eingesetzt, in denen keine personenbezogenen Daten verarbeitet werden. Da sie jedoch das Mittel der interoperablen Kommunikation darstellen, sind sie ein Bestandteil der gemeinsamen Datenverantwortlichkeit im Sinne dieser Vereinbarung.

## § 2

(1) Im Rahmen der gemeinsamen Verantwortlichkeit ist jeder Vereinbarungspartner für die Verarbeitung der personenbezogenen Daten bei dem bei ihm angelegten Nutzerkonto des Nutzers SK-N einschließlich der Basisdienste, insbesondere des Postfachs (Wirkbereich A), zuständig. Bei diesem Abschnitt wird der jeweils Verantwortliche als „Verantwortlicher SK-N“ bezeichnet. Gegenstand der Verarbeitung, deren Rechtsgrundlage § 8 OZG in der jeweils geltenden Fassung (oder seine Nachfolgevorschrift) ist, sind die in dieser Vorschrift genannten Daten. Die Interoperabilität der Nutzerkonten ist ein notwendiger Teil der OZG-Umsetzung. Die Vereinbarungspartner arbeiten gemeinsam an der Erstellung der Datenschutzhinweise und werden, falls zum Zeitpunkt der Produktivsetzung erforderlich, eine wirksame Einwilligung der Nutzer (Bürger) in die Verarbeitung ihrer personenbezogenen Daten an den Nutzerkonten einholen.

- (2) Ebenfalls ist jeder Vereinbarungspartner für die Verarbeitung der personenbezogenen Daten bei dem bei ihm zur Durchführung eines Fachverfahrens bestehenden Nutzerkonto einschließlich der Basisdienste, insbesondere des Postfachs (Wirkbereich B), zuständig. Gegenstand der Verarbeitung, deren Rechtsgrundlage § 8 OZG in der jeweils geltenden Fassung (oder seine Nachfolgevorschrift) ist, sind die in dieser Vorschrift genannten Daten. Die Interoperabilität der Nutzerkonten ist ein notwendiger Teil der OZG-Umsetzung. Die Vereinbarungspartner arbeiten gemeinsam an der Erstellung der Datenschutzhinweise und werden, falls zum Zeitpunkt der Produktivsetzung erforderlich, eine wirksame Einwilligung der Nutzer (Bürger) in die Verarbeitung ihrer personenbezogenen Daten an den Nutzerkonten einholen.
- (3) Der Betrieb der zentralen Komponenten fällt in den Wirkbereich der Organisationseinheit KIOSK (Wirkbereich C). Die datenschutzrechtliche Betrachtung gemäß Art. 26 DSGVO zum Schutz der Rechte des Nutzers bei der Verarbeitung seiner personenbezogenen Daten beschränkt sich in diesem Fall auf die einschlägigen Maßnahmen zur Erfüllung der Anforderungen entsprechend Art. 32 DSGVO.

### § 3

- (1) Jeder Vereinbarungspartner gewährleistet die Einhaltung der gesetzlichen Bestimmungen, insbesondere die Rechtmäßigkeit der durch ihn auch im Rahmen der gemeinsamen Verantwortlichkeit durchgeführten Datenverarbeitungen. Die Vereinbarungspartner ergreifen alle erforderlichen technischen und organisatorischen Maßnahmen, damit die Rechte der betroffenen Personen, insbesondere nach den Art. 12 bis 22 DSGVO, innerhalb der gesetzlichen Fristen jederzeit gewährleistet werden können bzw. sind.
- (2) Sind für die Geschäftsstelle Gründe für einen Verstoß gegen diese Vereinbarung erkennbar, informiert sie das Produktteam FINK.

### § 4

- (1) Betroffene Personen können die ihnen aus Art. 13 bis 22 DSGVO zustehenden Rechte gegenüber jedem der Vereinbarungspartner geltend machen.
- (2) Die Vereinbarungspartner sind sich einig, dass der „Verantwortliche SK-N“ die gemäß Art. 13 und 14 DSGVO erforderlichen Informationen zur Verarbeitung personenbezogener Daten im Wirkbereich A und der „Verantwortliche SK-VL“ die Informationen für die Verarbeitung der personenbezogenen Daten im Wirkbereich B bereitstellt.
- (3) Betrifft der geltend gemachte Anspruch des Betroffenen nicht den Wirkbereich des den Anspruch entgegengenommenen Partners, so leitet er ihn an den dafür jeweils verantwortlichen Vereinbarungspartner weiter, der die Beantwortung bzw. Bearbeitung und die Kommunikation mit dem Betroffenen übernimmt.

Betrifft der geltend gemachte Anspruch Wirkbereiche mehrerer Vereinbarungspartner, so sind diese verpflichtet, an der Beantwortung bzw. Bearbeitung zusammenzuwirken. Sie legen gemeinsam fest, wer die Kommunikation gegenüber dem Betroffenen übernimmt. Bei fehlender Einigung ist der Vereinbarungspartner verantwortlich, gegenüber dem der Anspruch zuerst geltend gemacht wurde.

Sollte ein Vereinbarungspartner für die Beantwortung bzw. Beantwortung eines Betroffenenbegehrens auf Informationen anderer Vereinbarungspartner angewiesen sein, stellen die angefragten Vereinbarungspartner die erforderlichen Informationen aus ihrem jeweiligen Wirkbereich zur Erfüllung des Betroffenenbegehrens zur Verfügung.

- (4) Für die Löschung personenbezogener Daten gemäß § 8 Abs. 1 OZG in der aktuellen Fassung bzw. gemäß der ihr nachfolgenden Norm ist der Vereinbarungspartner verantwortlich, in dessen Wirkbereich sich das fragliche Nutzerkonto befindet. Sollte eine betroffene Person einen darüberhinausgehenden Anspruch auf Löschung ihrer personenbezogenen Daten erheben, informiert der den Anspruch entgegennehmende Partner andere Vereinbarungspartner, deren Wirkbereiche betroffen sein könnten.

## § 5

Die Vereinbarungspartner informieren sich gegenseitig unverzüglich und vollständig, wenn sie bei der Prüfung der Verarbeitungstätigkeiten Fehler oder Unregelmäßigkeiten hinsichtlich datenschutzrechtlicher Bestimmungen feststellen, über diese Befunde.

## § 6

Allen Vereinbarungspartnern obliegen die aus Art. 33, 34 DSGVO resultierenden Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde und den von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen für ihren jeweiligen Wirkbereich. Die Vereinbarungspartner informieren sich unverzüglich gegenseitig über die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gemäß Satz 1 und leiten sich die zur Durchführung dieser Meldung erforderlichen Informationen jeweils unverzüglich zu.

## § 7

Dokumentationen im Sinne von Art. 5 Abs. 2 DSGVO, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, werden durch jeden Vereinbarungspartner entsprechend den rechtlichen Befugnissen und Verpflichtungen über das Vertragsende hinaus aufbewahrt.

## § 8

- (1) Die Vereinbarungspartner stellen innerhalb ihres Wirkbereiches sicher, dass alle mit der Datenverarbeitung befassten Mitarbeitenden die Vertraulichkeit der Daten gemäß den Artikeln 28 Abs. 3, 29 und 32 DSGVO für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses wahren und dass diese vor Aufnahme ihrer Tätigkeit entsprechend auf das Datengeheimnis verpflichtet bzw. hierzu belehrt sowie in die für sie relevanten Bestimmungen zum Datenschutz eingewiesen werden.
- (2) Die Vereinbarungspartner haben eigenständig dafür Sorge zu tragen, dass sie sämtliche in Bezug auf die Daten bestehenden gesetzlichen Aufbewahrungspflichten einhalten. Sie haben hierzu angemessene Datensicherheitsvorkehrungen (Art. 32 ff. DSGVO) zu treffen. Dies gilt insbesondere im Falle der Beendigung der Zusammenarbeit.

- (3) Die Implementierung, Voreinstellung und der Betrieb der IT-Komponenten sind unter Beachtung der Vorgaben der DSGVO und anderer Regelwerke, insbesondere unter Beachtung der Grundsätze des Datenschutzes durch Design und datenschutzfreundliche Voreinstellungen sowie unter Verwendung von dem Stand der Technik entsprechenden geeigneten technischen und organisatorischen Maßnahmen, durchzuführen.

## § 9

- (1) Die Vereinbarungspartner verpflichten sich, beim Einsatz von Auftragsverarbeitern im Anwendungsbereich dieser Vereinbarung, d.h. beim Betrieb von Nutzerkonten, einen Vertrag nach Art. 28 DSGVO abzuschließen oder durch ein anderes Rechtsinstrument im Sinne des Art. 28 Abs. 3 DSGVO sicherzustellen, dass insbesondere folgende Grundsätze gewährleistet werden:
- 1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt
  - 2) Der Betrieb der Nutzerkonten durch den Vereinbarungspartner im Sinne der Festlegungen des IT-Planungsrates, insbesondere der Entscheidung 2018/40 des IT-Planungsrates ist gewährleistet
  - 3) Dem Vereinbarungspartner stehen ausreichende Kontrollmöglichkeiten zu.  
Das Nähere kann die Geschäftsordnung regeln.

Mit der Erklärung des Beitritts muss der beitretende Vereinbarungspartner der Geschäftsstelle seinen im Sinne des § 9 Abs. 1 S. 1 beauftragten Auftragnehmer mitteilen und die Einhaltung der vorstehenden Grundsätze zusichern.

Die Vereinbarungspartner informieren sich gegenseitig rechtzeitig über jede beabsichtigte Änderung des nach den vorstehenden Sätzen beauftragten Auftragnehmers bzw. des für die Föderation FINK relevanten Datenverarbeitungsvorgangs.

Die Geschäftsstelle ist über den Vertragsschluss, den neuen Vertragspartner des Vereinbarungspartners und den wesentlichen Inhalt der Vereinbarung, sofern die Grundsätze des § 9 Abs. 1 S. 1 dieser Vereinbarung betroffen sind, zu informieren. Sind für die Geschäftsstelle Gründe erkennbar, weshalb das Einhalten der Grundsätze aus § 9 Abs. 1 S. 1 dieser Vereinbarung gefährdet sein könnte, informiert sie das Produktteam FINK.

- (2) Der Vereinbarungspartner stellt sicher, dass Subunternehmer in gleicher Weise wie der Hauptauftragnehmer die Anforderungen des Datenschutzrechts und die Festlegungen dieses Vertrages erfüllen. Nicht als Leistungen von Subunternehmern im Sinne dieser Regelung gelten Dienstleistungen, die die Vertragsparteien bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nehmen, beispielsweise Telekommunikationsdienstleistungen und Wartungen. Die Vereinbarungspartner sind jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der personenbezogenen Daten auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zur Erfüllung der Pflichten aus dieser Vereinbarung zu ergreifen.

## § 10

Unbeschadet der Regelungen dieses Vertrages haften die Vereinbarungspartner für den Schaden, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wird, im Außenverhältnis gemeinsam gegenüber den betroffenen Personen.

Im Innenverhältnis haften die Vereinbarungspartner, unbeschadet der Regelungen dieses Vertrages, nur für Schäden, die innerhalb ihres jeweiligen Wirkungsbereiches entstanden sind.