 

  DFN-CERT Services GmbH Logo

Checkliste-Informationsblatt

Gemeinsam Verantwortliche

nach Art. 26 EU-DSGVO

Version 1.0, 21. Februar 2019

Die Nutzung dieses Dokuments ist zulässig unter der Lizenz CC BY-SA 3.0    
<https://creativecommons.org/licenses/by-sa/3.0/de/legalcode>   
Autor: NRW Projektgruppe „Umsetzung der EU-Datenschutz-Grundverordnung (EU-DSGVO) −  
Datenschutzmanagementsysteme“ 2018

gefördert vom 

# Gemeinsam Verantwortliche nach Art. 26 EU-DSGVO

Oft sind an der Verarbeitung von personenbezogenen Daten auch externe Stellen beteiligt. Die Einbeziehung externer Stellen kann leider aus datenschutzrechtlicher Sicht nicht einheitlich behandelt werde. Je nachdem, wie die Zusammenarbeit bzw. Einbindung ausgestaltet ist, müssen unterschiedliche rechtliche Anforderungen eingehalten werden. Folgende Fälle mit mehreren Beteiligten sind zu unterscheiden:

# Gemeinsame Verantwortung

Hierbei tun sich mehrere Stellen zusammen, um gemeinsam personenbezogene Daten zu verarbeiten. Dies kann aus Gründen von Synergien oft Sinn machen. So ist es z.B. sinnvoll eine Forschungsdatenbank oder eine aufwendige Serverinfrastruktur gemeinsam zu betreiben. Voraussetzung für eine gemeinschaftliche Verantwortung ist, dass zwischen den beteiligten Partnern kein Über-/Unterordnungsverhältnis besteht. Prinzipiell muss somit jeder Partner neben dem gemeinsamen Zweck auch zumindest eine vertraglich garantierte Einflussmöglichkeit auf das Ob und Wie der Verarbeitung haben, wobei keine gleichen Einflussmöglichkeiten vorausgesetzt werden. Eine mögliche gemeinsame Verantwortung muss somit immer von einer alleinverantwortlichen Verarbeitung durch die jeweiligen Partner und von einer Auftragsverarbeitung abgegrenzt werden.

**Rechtsfolge:** Jeder Verantwortliche braucht seine eigene Rechtsgrundlage für die Verarbeitung, inklusive der Übermittlung an die anderen gemeinsam Verantwortlichen und kann sich somit nicht auf die einem anderen Partner zustehende Rechtsgrundlage mit berufen. Es muss zudem ein Vertrag zwischen den Beteiligten Partnern geschlossen werden, der die gemeinsame Verantwortlichkeit und die sich daraus ergebenden Rechte und Pflichten regelt. Eine Vorlage findet sich im Intranet der FH Bielefeld Die betroffenen Personen müssen im Rahmen der Informationspflichten über die gemeinsame Verarbeitung und die an dieser beteiligten Verantwortlichen informiert werden. Die DSK hält es für ausreichend, dass die Inhalte des Vertrags zwischen den Beteiligten veröffentlicht werden.

# Auftragsverarbeitung gem. Art. 28 EU-DSGVO

Bei der Auftragsverarbeitung wird eine externe Stelle in die eigene Verarbeitung eingebunden. Dies kann z.B. bei der Auslagerung des Serverbetriebs an eine andere Stelle der Fall sein. Der wesentliche Unterschied zur gemeinsamen Verantwortung besteht darin, dass der eigebundene Dienstleister einem umfänglichen Weisungsrecht des Auftraggebers unterliegt. Selbst wenn er entscheiden darf, von welchem Hersteller die Server bezogen werden, welchen Access-Provider und Stromanbieter er wählt: Der Auftraggeber kann ihm prinzipiell den Auftrag und die Daten entziehen. Bei der Auftragsverarbeitung besteht somit ein Über-/Unterordnungsverhältnis zwischen Auftraggeber und Auftragnehmer. Der Auftraggeber bleibt der alleinige Verantwortliche und unterstellt den Auftragnehmer seiner Kontrolle und seinen Anweisungen in Bezug auf die Verarbeitung der personenbezogenen Daten.

**Rechtsfolge:** Bei einer Auftragsverarbeitung gemäß Art. 28 DSGVO ist keine explizite Rechtsgrundlage für die Übermittlung der personenbezogenen Daten an den Auftragsverarbeiter erforderlich, weil die Daten auch dort weiter der alleinigen Verantwortung des Auftraggebers unterstehen. Auch hier muss ein Vertrag mit den inhaltlichen Mindestvoraussetzungen aus Art. 28 Abs. 3 DSGVO geschlossen werden, der die weitere Wahrnehmung der Verantwortlichkeit durch den Auftraggeber gewährleistet. Eine Vorlage befindet sich im Intranet der FH Bielefeld. Die betroffenen Personen müssen im Rahmen der Informationspflichten über die Einbindung des Auftragsverarbeiters informiert werden.

# Alleinverantwortliche Verarbeitung durch die externe Stelle

Von einer gemeinsamen Verantwortlichkeit abzugrenzen sind Fälle, in denen die externe Stelle die erhaltenen personenbezogenen Daten alleinverantwortlich verarbeitet. Dies ist dann der Fall, wenn mit der Verarbeitung kein gemeinschaftlicher Zweck, sondern ein eigener Zweck durch die externe Stelle verfolgt wird. Typische Beispielsfälle sind solche, in denen eine externe Stelle Daten bekommt um eine eigene Vertragsleistung weisungsfrei in eigener Verantwortung zu erbringen. Ein konkretes Beispiel ist die Fluggesellschaft, die Passagierdaten für die Erbringung der Beförderungsleistung benötigt. Es handelt sich nicht um eine Auftragsverarbeitung, weil die im Zusammenhang mit der Beförderung erfolgende Verarbeitung personenbezogener Daten frei von Weisungen des Auftraggebers erfolgt. Es handelt sich auch nicht um eine gemeinsame Verarbeitung. Zwar ist die Erbringung der vertraglichen Leistung auch im Interesse des Auftraggebers. Der Auftraggeber hat aber keinerlei Einfluss auf die Verarbeitung der personenbezogenen Daten im Rahmen der Erbringung. Auch wird trotz des bestehenden Interesses des Auftraggebers kein gemeinsamer Zweck verfolgt, da beide Vertragspartner auf unterschiedlichen Seiten des Vertrages stehen. Der Auftragnehmer verfolgt somit mit der Datenverarbeitung den Zweck der Erfüllung seiner Schuld gegenüber dem Auftraggeber. Dies ist somit nicht der gleiche Zweck, den der Auftraggeber verfolgt.

Auch bei gemeinsamen Verarbeitungen muss sauber abgegrenzt werden bis wohin der gemeinsame Zweck verfolgt wird und ab wann die Partner jeweils eigene Zwecke in alleiniger Verantwortung verfolgen.

**Beispiel:** Drei Hochschulen betreiben gemeinsam die Infrastruktur für ein Campus-Management. Soweit im Rahmen des gemeinsamen Betriebs personenbezogene Daten anfallen (z.B. Logdaten), erfolgt die Verarbeitung zum gemeinschaftlichen Zweck. Hinsichtlich der verarbeiteten Beschäftigen- und Studierendendaten wird jedoch jeweils eine alleinverantwortliche Verarbeitung durch die jeweilige Hochschule vorliegen, weshalb bezüglich dieser Daten auch eine Verarbeitung in getrennten Instanzen vorgesehen werden muss.

**Rechtsfolge:** Es ist eine explizite Rechtsgrundlage für die Übermittlung an die externe Stelle erforderlich. Die externe Stelle verarbeitet die Daten in alleiniger Verantwortung und aufgrund einer eigenen Rechtsgrundlage weiter. Die Übermittlung der personenbezogenen Daten an die externe Stelle muss der betroffenen Person im Rahmen der Informationspflichten transparent gemacht werden.

Die nachfolgende **Checkliste** soll die Feststellung vereinfachen, ob gegebenenfalls eine gemeinschaftliche Verantwortlichkeit für eine Datenverarbeitung nach Artikel 26 DSGVO oder einer der anderen Fälle vorliegt.

# Checkliste

*(Diese Checkliste soll systematisch die Bewertung ermöglichen, ob eine gemeinsame Verantwortlichkeit besteht)*

### Wer erhebt die personenbezogenen Daten? Liegt eine gemeinsame Erhebung vor?

**Wer erhebt die personenbezogenen Daten (Bitte nur Organisationen, Unternehmen nennen):**

|  |
| --- |
|  |

## **Bei Angabe mehrerer Stellen:** Liegt eine gemeinsame Erhebung der Daten vor (oder ist diese geplant) und ist diese für den Betrieb des Systems erforderlich?

Liegt eine gemeinsame Datenerhebung vor? Hauptindiz ist die Betroffenensicht: Tritt nur eine Stelle der betroffenen Person gegenüber auf oder mehrere (z.B. durch Nennung mehrerer Stellen auf einem Fragebogen)

**Ja**

Wenn ja, warum erfolgt dies gemeinschaftlich?

|  |
| --- |
|  |

**Hinweis zur Auswertung:** Bei einer begründeten gemeinsamen Datenerhebung liegt normalerweise eine gemeinsame Verarbeitung gem. Art. 26 DSGVO vor, da die Verfolgung eines gemeinsamen Zwecks mit gemeinsamen Mitteln naheliegt.

### Sind andere externe Stellen an der Verarbeitung der durch die Hochschule erhobenen Daten beteiligt?

*(****Erläuterung:*** *Externe Stellen sind auch An-Institute mit eigener Rechtsperson (z.B. GmbH, AG, e.V.). Eine Beteiligung liegt auch dann schon vor, wenn eine externe Stelle diese Daten erhält oder Einsicht in die Daten bekommt)*

|  |
| --- |
|  |

Hinweis zur Auswertung: Sind keine anderen Stellen beteiligt, liegt keine gemeinsame Verarbeitung, keine Auftragsverarbeitung und keine Übermittlung der Daten an einen anderen Verantwortlichen vor. Die Prüfung ist dann hier beendet.

### Dürfen die beteiligten externen Stellen selbst über die Art und Weise der Verarbeitung und die dabei verfolgten Zwecke entscheiden oder sind sie diesbezüglich an Weisungen der Hochschule gebunden?

*(****Erläuterung:*** *Darf die externe Stelle selbstbestimmt mit diesen Daten umgehen oder ist ihr dies nur im vertraglich vereinbarten Umfang erlaubt, wobei ihr die Hochschule jederzeit bindende Anweisung bis hin zur Untersagung der weiteren Verarbeitungen erteilen darf?****)***

Wenn Weisungsgebundenheit, bitte hier auflisten:

|  |  |  |
| --- | --- | --- |
| **Externe Stelle Datenempfänger** | **Weisungen**  **Ja/nein** | **Inhalt und Typ (schriftlich, mündlich, dauerhaft, übergangsweise, vertraglich, etc.) der Weisung (ggf. als Annex anzufügen)** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Hinweis zur Auswertung: Bei einer Weisungsgebundenheit der externen Stelle liegt in der Regel eine Auftragsverarbeitung durch die externe Stelle gegenüber der Hochschule vor. Eine Auftragsverarbeitung liegt in der Regel auch dann vor, wenn die externe Stelle noch selbst über die Mittel der Verarbeitung entscheiden kann, sofern sich die Hochschule die generelle Weisungsbefugnis vorbehält. Damit hat die Hochschule bei Einsatz eines inadäquaten Mittels immer noch die Möglichkeit, den Einsatz eines anderen Mittels zu verlangen oder die Verarbeitung bei der externen Stelle ganz zu beenden.

## Liegt ein Vertrag zur Auftragsverarbeitung (AV) vor?

***Zu beachten:*** *Das Bestehen eines Vertrags zur Auftragsverarbeitung ist nur ein Indiz für das Vorliegen einer Auftragsverarbeitung. Liegt keine Weisungsgebundenheit vor, handelt es sich um eine Verarbeitung als Verantwortlicher, egal ob ein Vertrag zur Auftragsverarbeitung besteht oder nicht. Man kann sich somit nicht durch die Wahl der Vertragsform aussuchen, Auftragsverarbeiter zu sein oder nicht. Entscheidend ist allein, ob aufgrund des Vertrags und der tatsächlichen Gegebenheiten eine eigenverantwortliche oder eine weisungsgebundene Verarbeitung erfolgt. Nur bei Weisungsgebundenheit liegt eine Auftragsverarbeitung vor. In diesem Fall müssen zwingend Verträge zur Auftragsverarbeitung geschlossen werden.*

**Bestehende Verträge mit den oben genannten externen Stellen:**

|  |  |  |
| --- | --- | --- |
| **Externe Stelle Datenempfänger** | **AV Ja/Nein** | **Bestehender AV-Vertrag Ja/Nein** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Hinweise zur Auswertung:**

**Besteht eine Auftragsverarbeitung** (weisungsgebundene Verarbeitung) und besteht noch kein Vertrag zur Auftragsverarbeitung, muss ein solcher mit der externen Stelle geschlossen werden. Bitte verwenden Sie in diesem Fall grundsätzlich die Vorlage aus dem Intranet der FH Bielefeld und nur ausnahmsweise mit vorheriger rechtlicher Überprüfung eine Vorlage der externen Stelle (zum hierfür vom Präsidium festgelegten Prozess s. Schreiben des Präsidiums vom 17.07.2018, veröffentlicht im Intranet der FH Bielefeld, hier findet sich auch eine Checkliste/Handreichung zur Prüfung). Die Prüfung ist für diese Fälle an dieser Stelle beendet.

**Besteht keine Auftragsverarbeitung**, muss eine weitere Prüfung erfolgen, egal ob eine Auftragsverarbeitungsvereinbarung besteht oder nicht. Aufgrund der fehlenden inhaltlichen Merkmale ist die externe Stelle Verantwortlicher. Es muss weiter geprüft werden, ob die externe Stelle die Daten in eigener oder gemeinsamer Verantwortung weiterverarbeitet.

### Erfolgt die Einbindung der externen Stelle aufgrund einer rechtlichen Verpflichtung oder um ihr eine Erfüllung einer vertraglich geschuldeten Leistung zu erfüllen, die sie in eigener Verantwortung erbringt?

(**Beispiele:** Die Hochschule ist aus dem Sozialrecht verpflichtet, an die gesetzlichen Krankenkassen Meldungen vorzunehmen. Die dortige Verarbeitung erfolgt in eigener Verantwortung der gesetzlichen Krankenkasse. Eine Fluggesellschaft benötigt die Passagierdaten, damit sie die Beförderungsleistung erbringen kann. Die damit zusammenhängende Verarbeitung erfolgt in alleiniger Verantwortung der Fluggesellschaft.

|  |  |  |
| --- | --- | --- |
| **Externe Stelle** | **Grund für die Einbindung ein eigenes Interesse der externen Stelle? Wenn ja, welches?** | **Weisungsgebunden bei der Ausführung Ja/Nein** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Hinweis zur Auswertung:** Die Annahme eines gemeinsamen Interesses kann nicht mit dem Interesse des anderen Vertragspartners an der Vertragserfüllung begründet werden. Es geht nicht um das Interesse an der Vertragserfüllung, sondern um die Verarbeitung der personenbezogenen Daten. Hier befinden sich die Vertragspartner auf zwei Seiten. Der Eine ist der Gläubiger der vertraglichen Leistung, der Andere der Schuldner. Benötigt der Schuldner personenbezogene Daten zur Erfüllung, erfolgt die diesbezügliche Verarbeitung nur in seinem Interesse und nicht in einem gemeinsamen Interesse. Folglich besteht in diesen Fällen auch keine gemeinsame Verantwortung für die Verarbeitung. Die Verantwortung liegt bei dem verarbeitenden Schuldner. Für die Übermittlung ist eine explizite Rechtsgrundlage erforderlich. Sollte die Weisungsgebundenheit bei der Ausführung bejaht werden, liegt wahrscheinlich eine Auftragsverarbeitung vor, die oben übersehen wurde.

### Existiert eine gemeinschaftliche Datenbank oder Speicherort der Daten, auf den alle Parteien vergleichbare (nahezu identische) Zugriffsrechte haben?

Z.B. eine gemeinsame Datenbank mit Forschungsdaten, auf die jeder beteiligte Partner zu seinen eigenen Forschungszwecken zugreifen darf.

|  |  |  |
| --- | --- | --- |
| **Verantwortliche Stelle, bei der Daten gehostet werden (bei Einschaltung eines Auftragsverarbeiters für das Hosting ist hier der Auftraggeber anzugeben)** | **Welche weiteren Stellen haben Zugriff? (Bitte hier jede Stelle einzeln aufführen)** | **Unter welchen Bedingungen erfolgt der Zugriff? (Bitte für jede in Spalte 2 genannte Stelle nennen)** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Hinweise zur Auswertung:** Bei Vorliegen dieser Voraussetzung liegt in der Regel eine gemeinsame Verarbeitung vor. Es muss ein entsprechender Vertrag über die gemeinsame Verarbeitung gemäß Art. 26 DSGVO geschlossen werden, wenn nicht bereits erfolgt. Erfolgt keine gemeinsame Erhebung (siehe ganz oben), muss diese gemeinsame Verarbeitung den betroffenen Personen bei der Erhebung durch die Informationen nach Art. 13 DSGVO transparent gemacht werden. Gleiches gilt, wenn die Daten ursprünglich zu einem anderen Zweck erhoben wurden und im Rahmen einer zulässigen Zweckänderung in die gemeinsame Datenbank eingebracht werden, soweit im Einzelfall keine Ausnahme von den Informationspflichten besteht.

### Besteht ein verbindender gemeinsamer Zweck in Bezug auf die Verarbeitung? Besteht zudem Einfluss auf das Wie (die Mittel) der Verarbeitung?

Um eine gemeinsame Verarbeitung von Verarbeitungen von Einzelverantwortlichen abzugrenzen, muss ein verbindender gemeinsamer Zweck feststellbar sein. Bei der Forschungsdatenbank ist dies z.B. die gemeinsame Datenhaltung, die im gemeinsamen Interesse vorgenommen wird. Werden Serversysteme an einer Stelle gemeinsam betrieben, dann ist die im Zusammenhang mit dem Serverbetrieb erfolgende Verarbeitung von personenbezogenen Daten der gemeinsame Zweck. Die (Mit-)Verantwortlichkeit setzt zudem grundsätzlich voraus, dass auch über die Mittel der Verarbeitung (mit-)bestimmt wird. Erfolgt der Betrieb nur durch einen der Verantwortlichen, schließt dies jedoch die Verantwortlichkeit der Anderen nicht aus, wenn diese zumindest vertraglich Interventionsmöglichkeiten eingeräumt bekommen, falls ein sicherer oder zuverlässiger Betrieb nicht gewährleistet ist.

|  |  |  |  |
| --- | --- | --- | --- |
| **Beteiligte Stellen** | **Abgrenzbarer gemeinsamer Zweck der Verarbeitung** | **Einflussmöglichkeiten auf den Betrieb Ja/Nein** | **Wie ist der Einfluss gewährleistet?** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Hinweise zur Auswertung:** Nur wenn diese Voraussetzungen gewährleistet sind, handelt es sich um eine gemeinsame Verarbeitung. Anderenfalls handelt es sich um Einzelverarbeitungen von Verantwortlichen.

# Anlage 1 – Wichtige Inhalte einer vertraglichen Vereinbarung über eine gemeinsame Verarbeitung

1. Definition des **gemeinsamen Zwecks** oder der gemeinsamen Zwecke der Datenverarbeitung
2. Festlegungen zu den **Mitteln** der Datenverarbeitung
   1. Wer übernimmt welche Aufgaben im Rahmen der gemeinsamen Verarbeitung?
   2. Festlegung bzw. Beschreibung der Speicherorte der Daten.
   3. Gegenseitige Unterstützung bei der Erstellung des Verzeichnisses der Verarbeitungen.
   4. Bei Schwerpunkt bei einem Partner: Vertragliche Festlegung der Einflussmöglichkeiten durch die anderen Partner.
   5. Wie erfolgt der interne Ausgleich, wenn der Aufwand für die Mittel nicht gleichmäßig verteilt ist? Werden gleiche Beiträge bezahlt und je nach Übernahme von Aufgaben ausgezahlt, oder findet ein anderweitiger Ausgleich bei Partnern mit höherem Aufwand statt?
   6. Gemeinsame Vorgaben zu technischen und organisatorischen Maßnahmen zur Gewährleistung des Schutzes von Personenbezogenen Daten und der Informationssicherheit.
   7. ggf. Ausschluss bestimmter Verarbeitungsmethoden (z.B. Automatische Entscheidungsfindung etc.) und Orte (z.B. EU-Ausland)
   8. Ausschluss von Zurückbehaltungsrechten an den personenbezogenen Daten.
3. Festlegung der **Kategorien der Personendaten und der Betroffenen**.
4. Festlegung, wer jeweils die Erfüllung der **Betroffenenrechte** übernimmt (Wichtig: diese Aufgabenteilung bindet nicht die betroffenen Personen, sondern nur die beteiligten Partner an der gemeinsamen Verarbeitung:
   1. Erfüllung der Informationspflichten: Der Regelfall wird sein, dass jeder Partner die bei ihm betroffenen Personen über die gemeinsame Verarbeitung informiert.
   2. Koordination von Anfragen durch betroffene Personen zwischen den Partnern und Klärung von Zuständigkeiten (inklusive Festlegung der Kontaktinformationen in den Datenschutzerklärungen)
   3. Soweit rechtlich und praktisch relevant: Festlegungen zur Erfüllung des Rechts auf Datenübertragbarkeit und deren technischer Umsetzung. Rechtlich relevant ist das Recht auf Datenübertragbarkeit nur bei einer Verarbeitung zur Durchführung eines Vertrags oder aufgrund einer Einwilligung. Selbst dann ist aber noch nach der praktischen Relevanz zu fragen. Nicht in jedem Fall eines rechtlich gegebenen Anspruchs besteht auch ein Interesse der betroffenen Personen an diesem Recht. Dies berechtigt zwar nicht zur Zurückweisung. Allerdings kann eine voraussichtlich niedrige praktische Relevanz (z.B. bei Forschungsprojekten) bei den Vorkehrungen berücksichtigt werden (z.B. Realisierungsmöglichkeit über Workarounds reicht aus).
   4. Gemeinsame Festlegung der Löschkriterien und -fristen.
5. **Schadensersatz**: Bei einer gemeinsamen Verarbeitung haften dem Geschädigten die Partner als Gesamtschuldner. Dies bedeutet, dass der Geschädigte von jedem Partner seinen ganzen Schaden ersetzt verlangen kann. Er kann sich somit den aus seiner Sicht solventesten Partner aussuchen. Dies lässt sich auch nicht zum Nachteil des Geschädigten anders regeln. Wenn ein Partner den ganzen Schaden bezahlen muss, ohne dass dieser gänzlich alleine für diesen Schaden verantwortlich ist, so hat dieser seinerseits Anspruch darauf, dass die auch verantwortlichen Partner ihren Teil übernehmen. Eine Vereinbarung sollte deshalb unbedingt eine Regelung dazu enthalten, dass der in Anspruch genommene Partner Anspruch auf Freihaltung hat, soweit die Verantwortung für den Schaden bei den anderen Partnern liegt. Zwar muss der in Anspruch genommene Partner zunächst einmal bezahlen, kann aber aufgrund der vertraglichen Vereinbarung von den anderen Partnern verlangen, dass diese ihren Anteil übernehmen.
6. Festlegung von Maßnahmen zur **Umsetzung von Meldepflichten** bei Datenschutzvorfällen:
   1. Die Partner verpflichten sich gegenseitig über Vorfälle unverzüglich zu informieren, bei denen personenbezogene Daten betroffen sind. Dies soll sicherstellen, dass jeder Partner seinen Meldepflichten gegenüber seiner Aufsichtsbehörde nachkommen kann.
7. Regelungen zur **Beendigung der gemeinsamen Verarbeitung**:
   1. Befristete oder unbefristete Laufzeit.
   2. Recht zur ordentlichen Kündigung (Das Recht zur außerordentlichen Kündigung besteht immer).
   3. Pflicht zur Herausgabe/Löschung der Daten des ausscheidenden Partners und die umgekehrte Pflicht des ausscheidenden Partners zur Herausgabe/Löschung der personenbezogenen Daten der anderen Partner.
   4. Ausschluss des Zurückbehaltungsrechts an personenbezogenen Daten.