# Verarbeitungsverzeichnis gemäß EU-Datenschutz-Grundverordnung

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-Datenschutz-Grundverordnung (DS-GVO).

## Namen und Kontaktdaten

**KATALYSE e.V.**
Beethovenstr. 6, 50674 Köln
Telefon: +49 (0)221 944048 0
Telefax: +49 (0)221 944048 9
E-Mail: info@katalyse.de

**Vorstand:**
Regine Rehaag
Telefon: +49 (0)221 944048 41
Handy: 015255181574
E-Mail: rehaag@katalyse.de

Frank Waskow
Telefon: +49 (0)221 944048 24
E-Mail: fwaskow@katalyse.de

**Systemadministrator, Datenschutz-Zuständiger**
Milan Stuhlsatz
E-Mail: stuhlsatz@katalyse.de

## Zwecke und Beschreibung der Verarbeitung – Art. 30 Abs. 1 S. 2 lit. B

- **Beschaffung/Einkauf sowie Finanzbuchhaltung**: Eingangsrechnungen (Einkauf von Produkten/Dienstleistungen), Ausgangsrechnungen und Mahnungen (Verkauf von Dienstleistungen), Korrespondenz mit Steuerberatung, Finanzamt und Banken
- **Erhebungen:** Daten von qualitativen und quantitativen Erhebungen (Befragungen, Interviews, Gruppendiskussionen): Erfassung und Verarbeitung von Daten für diverse Forschungszwecke.
- **Kooperationspflege**
- **Mitgliederverwaltung** (aktive Vereinsmitglieder und Fördermitglieder)
- **Personalverwaltung:**
  - Verarbeitung und Übermittlung von Daten für die Personalplanung, -anstellung, -entlohnung und die Personalentwicklung sowie die damit verbundene Verarbeitung und Übermittlung für Lohn-, Gehalts-, Entgeltabrechnung und Einhaltung von Arbeits- und sozialrechtlich vorgegebener Aufzeichnungs-, Auskunfts- und Meldepflichten, einschließlich erstellter und archivierter Textdokumente (z.B.: Bewerbungsschreiben, Dienstzeugnisse, Schriftverkehr mit Sozialversicherungsträgern) in diesen Angelegenheiten.
  - Arbeitszeiterfassung / Urlaubsdatei: Verarbeitung von Daten für die Erfassung von Arbeits- und Pausenzeiten und Urlaubstagen.

## Kategorien betroffener Personen und personenbezogener Daten - Art. 30 Abs. 1 S. 2 lit. c

Die betroffenen Personen wurden in Kategorien eingeteilt:

- Auftrag- und Fördergeber
- Auftragnehmer
  - Dienstleister
  - Lieferanten
- Forschungsteilnehmer_innen
- Kooperationspartner_innen
- Mitarbeitende
  - Angestellte
  - Freiwillige
- Mitglieder
  - Aktive Mitglieder
  - Fördermitglieder

## Kategorien von Empfängern - Art. 30 Abs. 1 S.2 lit. d

Die Empfänger von Daten wurden in Kategorien eingeteilt:

- Bank
- Finanzamt
- Sozialversicherungsträger
- Landschaftsverband Rheinland – LVR
- Bundesamt für zivilgesellschaftliche Angelegenheiten – BAfZA
- Forschungspartner
- Auftragnehmer
  - Transkriptionsbüros
  - Übersetzungsbüros
  - Steuerberatung

## Speicherdauer und Löschfristen - Art. 30 Abs. 1 S.2 lit. f

Mitgliederdaten werden bis zu zwei Jahre nach Beendigung der Vereinsmitgliedschaft gespeichert. Die restlichen Daten werden gemäß der gesetzlich festgelegten Fristen zehn Jahre lang aufbewahrt, darüber hinaus bis zur Beendigung eines eventuellen Rechtsstreits oder fortlaufender Gewährleistungs- oder Garantiefristen.

## Verzeichnis von Verarbeitungstätigkeiten

| Verarbeitungstätigkeit | Zwecke der Verarbeitung | Betroffene | Personenbezogene Daten | Empfänger | Löschfristen |
|---|---|---|---|---|---|
| Erhebung und Speicherung Personaldaten | Personalverwaltung | Mitarbeitende<br>– Angestellte<br>– Freiwillige | Name, E-Mail, Telefonnummer, Anschrift, Bankverbindung, Geburtsdatum, Familienstand, Konfession, Zahl der Kinder, Sozialversicherungs- und SteuerIdentnummer, Arbeitszeiten / Urlaubstage, Lohn-, Gehalts- und Entgeltabrechnung | LVR, BAfZA, Bank, Krankenkasse, Sozialversicherung, Steuerberatung, Finanzamt | zehn Jahre |
| | | Bewerber | Bewerbungsunterlagen | | umgehend nach Abschluss des Bewerbungsverfahrens |
| Erhebung und Speicherung Mitgliederdaten | Mitgliederverwaltung -kommunikation | Aktive Mitglieder | Name, Anschrift, Institution, Bankverbindung, E-Mail | Bank | 2 Jahre nach Austritt / Kündigung |
| | Mitgliederverwaltung | Fördermitglieder | Name, Anschrift, Institution, Bankverbindung | Bank | |
| Erhebung und Speicherung Daten Veranstaltungsteilnehmende | Veranstaltungsmanagement | Veranstaltungsteilnehmende | Name, Anschrift, Institution, E-Mail, Telefonnummer | - | umgehend nach Abschluss der Veranstaltung – sofern der Teilnehmende nicht um Informationen über weitere Veranstaltungen gebeten hat |

| | | | | | |
|---|---|---|---|---|---|
| Buchhalterische Erfassung Beschaffungs-/ Einkaufsdaten | Finanzbuchhaltung | Lieferanten, Dienstleister | Name, Anschrift, Institution, Bankverbindung, E-Mail, Telefonnummer | Steuerberatung, Finanzamt, Sozialversicherungsträger | 10 Jahre |
| Erhebung und Speicherung Kooperationspartnerdaten | Kooperation / Strategische Partnerschaften | Kooperationspartner_innen, Auftrag- und Fördergeber | Name, Anschrift, Institution, Bankverbindung, E-Mail, Telefonnummer | | 1 Jahr nach Ende der Kooperation |
| Erhebung und Speicherung von Daten aus wissenschaftlichen Erhebungen | Forschung | Forschungsteilnehmer_innen | qualitativen und quantitativen Daten, siehe 3.5 | Forschungspartner, Transkriptionsbüros | Mindestens zehn Jahre (vgl. Leitfaden zum Umgang mit Forschungsdaten, S. 8) |

# Technische und organisatorische Maßnahmen - Art. 30 Abs. 1 S. 2 lit. G

## Auftragsdatenverarbeitung

Werden im Rahmen eines Projektes personenbezogene Daten verarbeitet, wird nach § 11 des BDSG mit dem Auftraggeber ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen. Für die Einhaltung des Datenschutzes ist die wissenschaftliche Mitarbeiterin Janika Fitschen als Datenschutzbeauftragte in Kooperation mit dem Systemadministrator zuständig.

## 1. Pseudonymisierung personenbezogener Daten

Daten welche eine Identifikation der Forschungsteilnehmenden zulassen müssen bei Dateneingabe entweder umgehend vernichtet oder anonymisiert werden, dies bedeutet dass sie in pseudonymisierter Form gespeichert werden. Beispielweise wird

- in Transkripten allen Beiträgen einer Person derselbe Buchstabe anstelle des Namens verwendet.
- in Mehrfachbefragungen Daten welche eine Identifikation der Forschungsteilnehmen zulassen in gehashter Form gespeichert

Wenn Forschungsteilnehmende eingewilligt haben, noch einmal bei einer Folgeerhebung teilzunehmen dürfen die erforderlichen Kontaktdaten getrennt von den Erhebungsdaten bis zum Abschluss der letzten Folgeerhebung gespeichert werden.

## 2. Verschlüsselung personenbezogener Daten

Es wird je nach Kontext nach modernen Verschlüsselungsverfahren asymmetrisch oder symmetrisch verschlüsselt.

## 3. Gewährleistung der Vertraulichkeit der Systeme und Dienste

### 3.1. Zutrittskontrolle

Mit folgenden Maßnahmen wird Unbefugten der Zutritt zu Datenverarbeitungsanlagen, auf denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt: Die Vereinsräume befindet sich in der 1. Etage und sind über die allgemeine Haustür und über zwei Zugangstüren mit Zylinderschlössern gesichert. Die Schlüsselausgabe wird fortlaufend protokolliert und vom Empfänger unterzeichnet. Nur die Mitarbeitenden verfügen über Haus- und Büroschlüssel. Die Fenster werden nach Dienstschluss geschlossen, bei Terrassentür und Küchenfenster werden zudem die Rollladen herunter gelassen. Der Zugang zum Gebäudeschacht vor dem hinteren Bereich des Büros ist durch ein permanent abgeschlossenes Rolltor gesichert. Der Server befindet sich in einem eigenen Raum ohne Fenster mit einer abschließbaren Tür. Die Bürotüren und Fenster werden am Ende des Arbeitstages hinsichtlich sicheren Verschlusses überprüft, die Haustüren verschlossen. Die Haustür des Gebäudes ist ab 19.00 Uhr abgeschlossen.

### 3.2. Zugangskontrolle

Mit folgenden Maßnahmen wird die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert: Eine Software-Firewall überwacht den Datenverkehr zwischen Computer und verbundenen Netzwerken. Projekt- wie personenbezogenen Daten werden ausschließlich auf dem internen Server gesichert, es erfolgt grundsätzlich keine arbeitsplatzbezogene Speicherung. In einzelnen Fällen kann es notwendig sein, dass Mitarbeitende über das Internet auf Daten zugreifen können. In diesem Fall werden die Daten auf einer institutseigenen Softwareplattform auf Basis von ownCloud gespeichert. Diese ist auf deutschen Servern bei dem Anbieter All-inkl gehostet. Um den unberechtigten Zugriff dritter auf dort abgelegte Dateien zu verhindern, sind alle Daten ausschließlich in verschlüsselter Form gespeichert. Jeder Mitarbeitende verfügt über einen individuellen, durch ein Passwort geschützten Schlüssel. Daten sind grundsätzlich nur für ausgewählte Mitarbeitende verfügbar, wenn

dies für die Erfüllung ihrer Aufgaben für das Institut erforderlich ist. Die Verwaltung der Zugriffsberechtigungen erfolgt durch die Datenschutzzuständigen.

Für alle Mitarbeitenden ist ein personen- und aufgabenbezogenes Benutzerprofil eingerichtet (mit spezifischen Zugangsberechtigungen zu unterschiedlichen Laufwerken). Beim Login erfolgt für jeden Benutzer eine Passwortabfrage, dieses Passwort ist ausschließlich den Mitarbeitenden bekannt. Die Benutzerprofile werden vom Systemadministrator eingerichtet und mit einem „Erstpasswort" versehen. Die Mitarbeitenden werden anschließend aufgefordert ihr Passwort zu ändern. Der Systemadministrator kann auf Anfrage das Passwort zurücksetzen. Die Mitarbeitenden müssen in regelmäßigen Abständen ihr Passwort (die aus einer Kombination von Buchstaben und Ziffern, Groß- und Kleinschreibung inkl. Sonderzeichen bestehen und eine Mindestlänge besitzen) verändern. Der Zugang zu den vereinseigenen mobilen Computergeräten erfolgt in gleicher Weise, bei Außenterminen erfolgt die Sicherung der Daten nach Rückkehr in den Vereinssitz über den Server. Mobile Geräte und Datenträger werden nach modernen Verfahren (bspw. Veracrypt) verschlüsselt, um - insbesondere bei Verlust - Zugriff unberechtigter Dritter zu unterbinden und werden in einem abgeschlossenen Stahlschrank aufbewahrt.

**3.3. Zugriffskontrolle**

Mit folgenden Maßnahmen wird gewährleistet, dass die Mitarbeitenden ausschließlich auf diejenigen Daten zugreifen können, für die ihnen Zugriffsberechtigung eingeräumt wurde, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können: Der Datenzugriff für die einzelnen Nutzerkonten ist über einen Domainserver geregelt. Der Zugriff auf Verzeichnisse und Dateien erfolgt in Abstufungen. Für jedes Projekt wird in Abstimmung mit der Datenschutzbeauftragten und der jeweiligen Projektleitung ein Berechtigungskonzept erstellt. Der Systemadministrator vergibt danach die entsprechenden abgestuften Rechte. Es gibt Passwortrichtlinie die Aussagen macht zu Passwortlänge und Passwortwechsel (siehe 3.3.2. Zugangskontrolle). Externe Datenträger werden mit dem Programm „Bitlocker“ verschlüsselt. Es erfolgt eine ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) und es wird ein Aktenvernichter mit der Sicherheitsstufe intern (5mm) eingesetzt.

**3.4. Weitergabekontrolle**

Mit folgenden Maßnahmen wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung bzw. während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie überprüft werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist: Daten werden ausschließlich innerhalb der Vereinsräume bearbeitet. Die Zugriffskontrolle ist im Unterpunkt 3.3. beschrieben. Somit ist ein unbefugtes Lesen, Kopieren, Verändern oder Löschen der Daten ausgeschlossen. In Ausnahmefällen kann ein Austausch von personenbezogenen Daten mit Kooperationspartnern erforderlich sein. Die Übertragung der Daten an Kooperationspartner sowie der Empfang von personenbezogenen Daten erfolgen verschlüsselt über eine Webseite. Die Vereinseigenen Webseiten verwenden ein SSL Zertifikat. Erhobene Daten werden nur in anonymisierter oder pseudonymisierter Form weiter gegeben. Mit allen Kooperationspartnern des KATALYSE e.V. wird eine separate Datenschutzvereinbarung geschlossen. Transportpersonal und –fahrzeuge werden bei physischem Transport sorgfältig ausgesucht.

**3.5. Trennungskontrolle**

Mit folgenden Maßnahmen wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können: personenbezogene und untersuchungsbezogene Erhebungsunterlagen werden in den Vereinsräumen getrennt voneinander aufbewahrt. Die eingegebenen Daten werden Projektbezogen separat gespeichert, personenbezogene Daten unmittelbar nach der Auftragsverarbeitung gelöscht. Soweit in einem Projekt personenbezogene Daten erhoben und weiterverarbeitet werden, ist der Umgang mit diesen Daten ausschließlich der Projektleitung und den schriftlich dazu autorisierten Projektmitarbeitenden gestattet. Eine Liste der Personen, die mit per-

sonenbezogenen Daten umgehen, wird dem Auftraggeber auf Nachfrage schriftlich vorgelegt. Dateien zur Entschlüsselung von pseudonymisierten Daten liegen auf einem externen, gesicherten IT-System. Produktiv- und Testsysteme sind voneinander getrennt.

## 4. Gewährleistung der Integrität der Systeme und Dienste

### 4.1. Eingabekontrolle

Mit folgenden Maßnahmen wird gewährleistet, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können: Eingabe, Änderung und Löschung von Daten werden entsprechend der gängigen DSGVO-Richtlinien protokolliert. Eine Überprüfung und Speicherung von Eingaben, Veränderungen bzw. Löschungen aus Standard Office Anwendungen (Word, Excel oder PowerPoint Dateien) heraus erfolgt nicht. Der Zugriff auf sämtliche relevanten Verzeichnisse und Daten sind unter dem Punkt Zugriffskontrolle beschrieben. Das Löschen von Daten durch Unbefugte ist aufgrund der existierenden Rechtevergabe ausgeschlossen.

## 5. Gewährleistung der Verfügbarkeit der Systeme und Dienste

### 5.1. Auftragskontrolle

Mit folgenden Maßnahmen wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können: Der KATALSE e.V. verwendet zur Verfügung gestellte Daten ausschließlich im Rahmen des jeweiligen Auftrags. Alle Mitarbeitenden sind mit den für Sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und auf das Datengeheimnis i. S. d. § 5 BDSG verpflichtet worden. Etwaige Auftragnehmer und deren Projektleitung sichern ferner zu, dass die mit der Durchführung der Arbeiten beschäftigten Personen, mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und auf das Datengeheimnis i. S. d. § 5 BDSG verpflichtet werden.

### 5.2. Verfügbarkeitskontrolle

Mit folgenden Maßnahmen wird gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind: Der Serverraum liegt über der Wassergrenze und außerhalb eines Hochwassergebiets. Es erfolgt eine regelmäßige Datensicherung auf eine externe Festplatte und die Datensicherung und –wiederherstellung wird regelmäßig überprüft und getestet. Der Server ist mit einer unterbrechungsfreien Stromversorgung (USV) ausgestattet. Es findet eine regelmäßige proaktive Wartung aller IT-Systeme statt. Durch wöchentliche Serverbackups auf externe Festplatten ist gesichert, dass im Falle eines Ausfalls des Servers Daten wiederhergestellt werden können.

## 6. Gewährleistung der Belastbarkeit der Systeme und Dienste

Der Datenschutzzuständige

- kontrolliert regelmäßig die Funktionsfähigkeit der Systeme,
- stellt sicher, dass die Software regelmäßig aktualisiert wird und
- ausreichend Speicherplatz auf den verwendeten Datenträgern zur Verfügung steht

## 7. Wiederherstellung personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Die Verfügbarkeit von personenbezogenen Daten wird durch wöchentliche, manuelle Server-Backups gewährleistet. Die Festplatte, auf der sich die Backups befinden, wird in einem abgeschlossenen Stahlschrank aufbewahrt. Um zu gewährleisten, dass die Backups korrekt ausgeführt werden, wird das „Vier-Augen-Prinzip“ angewendet. Erst wenn zwei Mitarbeiter die gesicherten Daten kontrolliert haben und der ausführende Mitarbeiter sich in einer Liste eingetragen hat, ist der Backupvorgang korrekt abgeschlossen.

### 8. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

## Anhang

### Leitfaden zum Umgang mit Forschungsdaten

Forschungsdaten sind Daten, die im Verlauf eines wissenschaftlichen Arbeitsprozesses erzeugt und verarbeitet werden. Sie bilden die Grundlage von Forschungsergebnissen. Dabei kann es sich um sehr unterschiedliche Arten von Daten handeln, z.B. um Messergebnisse, Sekundäranalysen, Visualisierungen, Modelle oder die Resultate von Umfragen und Erhebungen. Ebenso vielfältig sind die möglichen Datei-Formate, die auf Zahlen, Text, Programmcode oder Grafik basieren können.

Es gehört zur guten wissenschaftlichen Praxis, zumindest die Forschungsdaten, die die Grundlage publizierter Arbeiten bilden, für **mindestens zehn Jahre** aufzubewahren. Im Sinne der einfachen Nachprüfbarkeit von Ergebnissen sowie zur Nachnutzung sollte angestrebt werden, möglichst viele Daten öffentlich zugänglich zu machen, sie also zu publizieren. Öffentliche Förderer und große internationale Zeitschriften verlangen dies in zunehmendem Maße.

Damit Forschungsdaten sinnvoll nachgenutzt werden können, aber auch, um ihre Erstbearbeitung und Analyse am Ende eines längeren Projektes zu erleichtern, sollte unbedingt bereits zu Beginn eines Projektes der Umgang mit Daten erörtert und in Form eines Datenmanagementplans schriftlich festgehalten werden. Dazu gehören z.B. auch Überlegungen zur systematischen Ablage und Benennung von Dateien. Sicherheitsaspekte, Datenschutz, Zugriffsrechte und Backup-Strategien sollten ebenfalls frühzeitig durchdacht werden. Bei der Publikation ist darauf zu achten, dass eine eindeutige Identifizierung der Datensätze und somit ihre Zitierbarkeit sichergestellt ist, z.B. mithilfe eines "Digital Object Identifiers" (DOI).

In welchem Umfang Sie Angaben zum Umgang mit Forschungsdaten machen müssen, hängt von der jeweiligen Ausschreibung, Ihrem Fach und der Art der in Ihrem Projekt erhobenen Daten ab. Beispielsweise hat das BMBF für den Bereich Empirische Bildungsforschung eine eigene Checkliste herausgegeben. In jedem Fall sollten Sie darlegen, wie Sie Ihre Daten gemäß der guten wissenschaftlichen Praxis für **mindestens zehn Jahre** aufbewahren (Empfehlung 7). In der Regel erwartet der Förderer auch, dass Sie Ihre Forschungsdaten nach Projektabschluss öffentlich zur Verfügung stellen, sofern dem keine rechtlichen Gründe (Datenschutz, Patentrecht, vertragliche Vereinbarungen mit Industriepartnern, etc.) entgegenstehen. Das wiederum setzt eine angemessene Aufbereitung voraus. (vgl. https://www.fdm.uni-hannover.de/fdm-leitfaden.html).