Datenschutz-Leitfaden für Begünstigte in den EU-Programmen Erasmus+ und Europäisches Solidaritätskorps (ESK)

Der Schutz personenbezogener Daten hat in den vergangenen Jahren stark an Bedeutung gewonnen. Der sensible Umgang mit personenbezogenen Daten spielt auch in der aktuellen Programmgeneration von Erasmus+ und Europäisches Solidaritätskorps eine bedeutende Rolle. Grundlage hierfür bildet die EU-Datenschutz-Verordnung 2018/1725 der Europäische Kommission, die in allen Finanzhilfevereinbarungen Erwähnung findet.

Als Vertragspartner haben Sie bei der Verarbeitung personenbezogener Daten in Erasmus+ und ESK die Rolle der „auftragsverarbeitenden" Organisation. Daraus ergeben sich während der Durchführung Ihrer Projekte unter anderem folgende Verpflichtungen: die Gewährleistung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten, die Benachrichtigung der Programmteilnehmenden über die Verarbeitung ihrer personenbezogenen Daten sowie das Führen von Verarbeitungsverzeichnissen (zum Beispiel in Form einer Tabelle, in der alle Verarbeitungstätigkeiten aufgelistet sind).

Zum besseren Verständnis hat die Europäische Kommission einen Leitfaden erstellt, der die datenschutzrelevanten Verpflichtungen transparent und übersichtlich darstellt. Im ersten Teil werden die Verpflichtungen aufgelistet, die sich aus der Rolle als auftragsverarbeitende Organisation für Sie ergeben. Der zweite Teil enthält eine Sicherheits-Checkliste mit den wichtigsten Maßnahmen zur Sicherstellung des Schutzes personenbezogener Daten. Im dritten Teil werden die Rollen der beteiligten Akteure zum Thema Datenschutz erläutert. Im vierten Teil finden Sie eine Tabelle, die Sie als Vorlage verwenden können, um Ihre Verarbeitungstätigkeiten zu dokumentieren (Verarbeitungsverzeichnis).

Im Auftrag der Europäischen Kommission bitten wir Sie als Begünstigte um Beachtung dieses Leitfadens.

Übersicht

Teil I: Was bedeutet es für Begünstigte, Auftragsverarbeitende personenbezogener Daten in den Programmen Erasmus+ und Europäisches Solidaritätskorps zu sein?

1. **Handeln auf Veranlassung**: Sie dürfen personenbezogene Daten nur zu den Zwecken verarbeiten, die in der hier verfügbaren Datenschutzerklärung genannt sind: https://webgate.ec.europa.eu/erasmus-esc/index/privacy-statement. Wenn Sie die Daten für Ihre eigenen Zwecke verarbeiten, handeln Sie nicht mehr als Auftragsverarbeitende, sondern werden für diese Verarbeitungstätigkeit zur datenverantwortlichen Organisation. Die wichtigsten Akteure sind im weiteren Verlauf dieses Dokuments beschrieben.

2. **Vertraglich gebunden:** Sie haben eine Finanzhilfevereinbarung mit der E+- oder ESK-Nationalagentur abgeschlossen, in der Ihre Pflichten als Auftragsverarbeitende beschrieben sind. Dieser Vertrag legt die rechtlichen Rahmenbedingungen für Ihre Rolle als Auftragsverarbeitende gemäß der Verordnung 2018/1725 fest, in der die Pflichten der Auftragsverarbeitenden in Artikel 29 beschrieben sind.

3. **Einsatz von Unterauftragsverarbeitenden**: Ohne vorherige schriftliche Genehmigung durch die datenverantwortliche Organisation dürfen Sie keine weiteren Verarbeitenden beauftragen. Bitte wenden Sie sich für weitere Informationen zu diesem Thema an die datenverantwortliche Organisation. Die Kontaktdaten finden Sie in der Datenschutzerklärung. Bitte setzen Sie Ihre Nationalagentur bei einer Kontaktaufnahme in Kopie.

4. **Umsetzung von Datensicherheit**: Sie müssen technische und organisatorische Maßnahmen ergreifen, die dem Risiko der Verarbeitung entsprechen, um den Schutz personenbezogener Daten sicherzustellen. Dies schließt Schutzmaßnahmen vor versehentlicher oder unrechtmäßiger Zerstörung sowie Verlust, Veränderung, unbefugte Offenlegung oder unerlaubte Zugriffe auf die Daten ein (siehe Sicherheits-Checkliste weiter unten).

5. **Meldung von Verletzungen des Schutzes personenbezogener Daten:** Sie müssen die datenverantwortliche Organisation unverzüglich informieren, wenn Sie von Verletzungen des Schutzes personenbezogener Daten erfahren. Sie müssen die datenverantwortliche Organisation außerdem bei der Pflichterfüllung im Zusammenhang mit Verletzungen des Schutzes personenbezogener Daten unterstützen, indem Sie alle erforderlichen Informationen über den Vorfall und bereits ergriffene Maßnahmen zur Eindämmung des Schadens zur Verfügung stellen und die möglichen Konsequenzen für die betroffenen Personen einschätzen. Die Kontaktdaten der datenverantwortlichen Organisation finden Sie in der Datenschutzerklärung. Bitte setzen Sie Ihre Nationalagentur bei einer Kontaktaufnahme in Kopie.

6. **Meldung von möglichen Datenschutzverletzungen:** Sie müssen unverzüglich die daten-verantwortliche Organisation informieren, wenn der Zweck und die Methoden der Verarbeitung einen Verstoß gegen die Verordnung (EU) 2018/1725 oder Ihre nationalen Datenschutzgesetze darstellen würden.

7. **Rechenschaftspflicht**: Sie müssen Ihre Rechenschaftspflichten einhalten, wie zum Beispiel die Erstellung und Umsetzung von Datenschutzrichtlinien (Richtlinien zur Standardisierung der Verwendung, Überwachung und Verwaltung personenbezogener Daten in Ihrer Organisation), sowie die Dokumentation Ihrer Verarbeitungstätigkeiten (siehe beigefügte Vorlage als Beispiel für die Dokumentation der Kategorien der Verarbeitungstätigkeiten).

8. **Einschränkung der Übertragung ins Ausland:** In der Datenschutzverordnung sind sehr strenge Regeln für die Übertragung personenbezogener Daten in Drittstaaten festgelegt. Sie müssen sicherstellen, dass der Datenverantwortliche die Übertragung in Länder außerhalb der EU / des EWR genehmigt hat, die über die in der Finanzhilfevereinbarung mit der E+- oder ESK-Nationalagentur beschriebenen Übertragung hinausgeht, und dass bei der Übertragung die Vorschriften der Verordnung bezüglich des internationalen Datentransfers eingehalten werden. Dies bezieht sich auf Situationen, in denen Sie Daten direkt und ohne die IT-Tools der Europäischen Kommission an andere Organisationen außerhalb der EU / des EWR übermitteln oder in denen Sie solchen Organisationen über die IT-Tools der Europäischen Kommission Zugriff gewähren. Bitte wenden Sie sich für weitere Informationen zu diesem Thema an die datenverantwortliche Organisation. Die Kontaktdaten finden Sie in der Datenschutzerklärung. Bitte setzen Sie Ihre Nationalagentur bei einer Kontaktaufnahme in Kopie.

Teil II: Sicherheits-Checkliste

- **Wir verstehen die Anforderungen an Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit** von Systemen und Diensten, in denen Daten verarbeitet werden.

    - **Vertraulichkeit** dient dem Schutz der Privatsphäre. Vertraulichkeitsmaßnahmen sollen sensible Informationen vor unbefugten Zugriffsversuchen schützen.

    - **Integrität** bedeutet, dass die Konsistenz, Korrektheit und Glaubwürdigkeit der Daten während der gesamten Nutzungsdauer erhalten bleiben. Daten dürfen während einer Übertragung nicht verändert werden, und Sie müssen Maßnahmen ergreifen, um sicherzustellen, dass die Daten nicht durch Unbefugte verändert werden können (z.B. durch Verletzung der Vertraulichkeit).

- **Verfügbarkeit** bedeutet, dass die Information für befugte Parteien konsistent und einfach zugänglich sein sollte. Das bedeutet, dass Hardware, technische Infrastruktur und Systeme, die die Daten speichern und anzeigen, angemessen gewartet werden müssen.

- **Ausfallsicherheit** bezieht sich auf die Fähigkeit Ihrer Organisation, den Betrieb während einer Unterbrechung aufrecht zu erhalten, und auf ihre Fähigkeit, die Systeme "rechtzeitig" in einen funktionsfähigen Zustand zurückzuversetzen.

- **Wir wissen, wer Zugriff auf unsere Daten hat**, und überprüfen regelmäßig die Liste der befugten Personen – dies gilt sowohl für die von der Europäischen Kommission bereitgestellten als auch für die von uns verwendeten IT-Tools. Die befugten Personen unterliegen einer entsprechenden gesetzlichen Verschwiegenheitspflicht.

- **Wir übermitteln Daten nur über sichere Übertragungsprotokolle** (z.B.: sichere Internet-Browser-Verbindungen, keine unverschlüsselten E-Mails)

- **Wir speichern Daten an sicheren Orten,** wenn wir die Daten aus den IT-Tools der Europäischen Kommission exportieren und stellen sicher, dass nur befugtes Personal Zugriff hat (gute Beispiele: lokales Laufwerk eines passwortgeschützten Computers, Netzlaufwerk (Dateiserver) mit Zugriffskontrolle; schlechte Beispiele: lokales Laufwerk eines öffentlich verfügbaren Computers, ein USB-Laufwerk, Cloud-Speicher - soweit nicht aufgrund der Sicherheitsrichtlinien Ihrer Organisation gestattet).

- **Wir sind uns der begrenzten Aufbewahrungsfrist für Daten bewusst** und stellen die Verarbeitung personenbezogener Daten für die in der Datenschutzerklärung beschriebenen Zwecke außerhalb der von der Europäischen Kommission bereitgestellten IT-Tools ein, sobald die Frist abgelaufen ist.

Teil III: Wer sind die wichtigsten Akteure bei der Verarbeitung personenbezogener Daten in den Programmen Erasmus+ und dem Europäischen Solidaritätskorps?

Für die in der Datenschutzerklärung unter https://webgate.ec.europa.eu/erasmus-esc/index/privacy-statement definierten Verarbeitungstätigkeiten:

1. Die Generaldirektion Bildung, Jugend, Sport und Kultur der Europäischen Kommission agiert als **die datenverantwortliche Organisation**.

2. Die E+- und ESK-Nationalagenturen agieren als **Auftragsverarbeitende**.

3. Organisationen und Einzelpersonen, die eine Finanzhilfevereinbarung mit den E+- und ESK-Nationalagenturen unterzeichnen und daraus resultierende Rechte und Pflichten übernehmen, agieren als **Auftragsverarbeitende** (auch Unterauftragsverarbeitende genannt).

Teil IV: Verarbeitungsverzeichnis

Gemäß Artikel 31 Absatz 2 der Datenschutz-Verordnung (EU) 2018/1725 haben Sie als Vertragspartner im Umgang mit personenbezogenen Daten in Erasmus+ und ESK die Verpflichtung, ein sogenanntes Verarbeitungsverzeichnis zu führen. Darin müssen Sie Ihre konkreten Verarbeitungsvorgänge erfassen. Eine Vorlage in Tabellenform, die die Anforderungen der Verordnung erfüllt, finden Sie anbei: Vorlage zur Dokumentation von Verarbeitungstätigkeiten (Verarbeitungsverzeichnis)