

Auftragsverarbeitung Foto

Anlage zum Honorarvertrag Foto Nr. XX/19

- Die **DKJS** wird in dieser Anlage als „**Auftraggeberin**“ bezeichnet und ist die „verantwortlich Stelle“ im Sinne der Datenschutzgrundverordnung (DSGVO).
- Der/die **Fotograf*in** wird als „**Auftragnehmer*in**“ bezeichnet und ist „Auftragsverarbeiter*in“ im Sinne der DSGVO.

Die Vertragspartner haben den o.g. Honorarvertrag über fotografische Dienstleistungen geschlossen. Dabei verarbeitet der/die Auftragnehmer*in personenbezogene Daten für die Auftraggeberin in deren Auftrag und nach deren Weisung im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO (sog. Auftragsverarbeitung). Diese Anlage konkretisiert die sich daraus ergebenden Verpflichtungen zum Datenschutz. Die Anlage wird Vertragsbestandteil und nicht gesondert unterschrieben.

1. Ort der Datenverarbeitung

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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2. Gegenstand der Datenverarbeitung

Es werden personenbezogene Daten in Form von Fotos verarbeitet.

3. Betroffene Personen

Von der Verarbeitung betroffen ist folgender Personenkreis:

- an Veranstaltungen oder Projekten der Auftraggeberin teilnehmende Kinder, Jugendliche und Erwachsene,
- Vortragende auf Veranstaltungen der Auftraggeberin,
- Mitarbeitende der Auftraggeberin.

4. Technisch-organisatorische Maßnahmen

(1) Der/die Auftragnehmer*in hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und der Auftraggeberin auf Anforderung zur Prüfung zu übergeben.

(2) Der/die Auftragnehmer*in hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Vorkehrungen um Maßnahmen der Datensicherheit zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen (Einzelheiten s. Anlage).

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insofern ist es dem/der Auftragnehmer*in gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5. Berichtigung, Einschränkung und Löschung von Daten

(1) Der/die Auftragnehmer*in darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung der Auftraggeberin berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den/die Auftragnehmer*in wendet, wird der/die Auftragnehmer*in dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Daten-Portabilität und Auskunft nach dokumentierter Weisung der Auftraggeberin unmittelbar durch den/die Auftragnehmer*in sicherzustellen.

6. Qualitätssicherung und sonstige Pflichten des/der Auftragnehmer*in

Der/die Auftragnehmer*in hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben. Der/die Auftragnehmer*in...

- a) fungiert als Ansprechpartner*in für datenschutzrechtliche Belange,
- b) setzt gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der/die Auftragnehmer*in und jede ihm/ihr unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung der Auftraggeber*in verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind,

- c) setzt alle für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO um (Einzelheiten s. Anlage).
- d) arbeitet auf Anfrage der Auftraggeber*in mit der Aufsichtsbehörde mit zusammen, wenn und soweit es um die Erfüllung der Aufgaben aus diesem Vertrag geht,
- e) informiert unverzüglich die Auftraggeberin über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim dem/der Auftragnehmer*in ermittelt.
- f) unterstützt die Auftraggeberin nach besten Kräften, soweit die Auftraggeberin ihrerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines/einer Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei dem/der Auftragnehmer*in ausgesetzt ist,
- g) kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem/ihrem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird,
- h) weist die getroffenen technischen und organisatorischen Maßnahmen gegenüber der Auftraggeberin im Rahmen derer Kontrollbefugnisse nach Ziffer 8 dieses Vertrages nach.

7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der/die Auftragnehmer*in z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der/die Auftragnehmer*in ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten der Auftraggeberin auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der/die Auftragnehmer*in darf Unterauftragnehmer*innen (weitere Auftragsverarbeitung) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung der Auftraggeber*in beauftragen. Ohne Zustimmung der Auftraggeber*in ist eine Unterbeauftragung unzulässig.

8. Kontrollrechte der Auftraggeberin

(1) Die Auftraggeber*in hat das Recht, im Benehmen mit dem/der Auftragnehmer*in Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer*innen durchführen zu lassen. Sie hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den/die Auftragnehmer*in in dessen/deren Geschäftsbetrieb zu überzeugen.

(2) Der/die Auftragnehmer*in stellt sicher, dass sich die Auftraggeberin von der Einhaltung der Pflichten des Auftragnehmers/der Auftragnehmerin nach Art. 28 DS-GVO überzeugen kann. Der/die Auftragnehmer*in verpflichtet sich, der Auftraggeberin auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Für die Ermöglichung von Kontrollen durch die Auftraggeberin kann der/die Auftragnehmerin einen Vergütungsanspruch geltend machen.

9. Mitteilung bei Verstößen des Auftragnehmers/der Auftragnehmerin

(1) Der/die Auftragnehmer*in unterstützt die Auftraggeberin bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an die Auftraggeberin zu melden
- die Verpflichtung, die Auftraggeberin im Rahmen ihrer Informationspflicht gegenüber Betroffenen zu unterstützen und ihr in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung der Auftraggeberin für deren Datenschutz-Folgenabschätzung
- die Unterstützung der Auftraggeberin im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers/der Auftragnehmerin zurückzuführen sind, kann der/die Auftragnehmer*in eine Vergütung beanspruchen.

10. Weisungsbefugnis der Auftraggeberin

(1) Mündliche Weisungen bestätigt die Auftraggeberin unverzüglich (mind. Textform).

(2) Der/die Auftragnehmer*in hat die Auftraggeberin unverzüglich zu informieren, wenn er/sie der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der/die Auftragnehmer*in ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Auftraggeberin bestätigt oder geändert wird.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen der Auftraggeberin nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch die Auftraggeberin – spätestens mit Beendigung der Leistungsvereinbarung – hat der/die Auftragnehmer*in sämtliche in seinen/ihren Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, der Auftraggeberin auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den/die Auftragnehmer*in entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er/Sie kann sie zu seiner/ihrer Entlastung bei Vertragsende der Auftraggeberin übergeben.

Anlage – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkenschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle: Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO): Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle: Keine Auftragserarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggeberin, eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.