Datenschutzrichtlinie

All3DP GmbH

Ridlerstr. 31A
D - 80339 München

November 2020

Datenschutzrichtlinie All3DP GmbH

Inhalt

Datenschutzrichtlinie All3DP GmbH

Vorwort der Geschäftsleitung

Die All3DP GmbH ist als global tätiges Unternehmen zur Einhaltung von Datenschutzrechten der Bundesrepublik Deutschland, der Europäischen Union und weltweit verpflichtet.

Das Unternehmen bietet über seine Websites redaktionelle Inhalte und Kaufempfehlungen rund um den 3D-Druck-Markt an und stellt seinen Besuchern eine Plattform zur Vermittlung von Druckaufträgen in diesem Umfeld bereit.

Dabei verarbeitet die All3DP die Daten der Websitebesucher und Plattformnutzer, welche ggf. auch Rückschlüsse auf deren Verhalten und Lebensumfeld zulassen können.

Seit Mai 2018 ist die Europäische Datenschutzgrundverordnung vollumfänglich gültig und ist neben einigen wenigen nationalen Regelungen die Grundlage für die Verarbeitung personenbezogener Daten für alle Bewohner der Europäischen Union und auch über die Ländergrenzen hinweg.

Daher ist es für die Geschäftsführung selbstverständlich eine Datenschutzrichtlinie zu erstellen, welche es allen Mitarbeitern und Partnern ermöglicht, sich bei der Verarbeitung von personenbezogenen Daten sicher zu bewegen und die Risiken für die Betroffenen richtig einschätzen zu können.

Die Geschäftsleitung steht hinter dieser Richtlinie.

Alle Mitarbeiter und Partner sind deshalb ebenfalls angehalten, diese Richtlinie bei ihrer täglichen Arbeit zu leben und umzusetzen.

Für die Geschäftsführung

Matthias Plica, CEO

Datenschutzrichtlinie All3DP GmbH

Geltungsbereich und Ziele

Die All3DP GmbH (All3DP) verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten, der Bundesrepublik Deutschland, der Europäischen Union und weltweit.

Diese Datenschutzrichtlinie gilt primär für alle Mitarbeiter und Partner des Unternehmens.

Sie beruht auf den europäischen Grundprinzipien zum Datenschutz und erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten. In Ländern, in denen Daten juristischer Personen in gleicher Weise wie personenbezogene Daten geschützt werden, gilt diese Datenschutzrichtlinie auch in gleicher Weise für Daten juristischer Personen. Anonymisierte Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzrichtlinie.

Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation von All3DP als attraktiver Arbeitgeber.

Sie gewährleistet das von der Europäischen Datenschutzverordnung (DSGVO) und den nationalen Gesetzen verlangte angemessene Datenschutzniveau (BDSG-neu) auch für den grenzüberschreitenden Datenverkehr in solche Länder, in denen gesetzlich kein angemessenes Datenschutzniveau besteht.

Eine Änderung dieser Datenschutzrichtlinie findet in Abstimmung mit dem Datenschutzbeauftragten statt.

Die aktuellste Version der Datenschutzrichtlinie kann unter der Rubrik „Datenschutz“ auf der Internetseite von All3DP jederzeit abgerufen werden.

Die Datenschutzrichtlinie regelt den allgemeinen Umgang mit personenbezogenen Daten im Unternehmen und wird ergänzt um konkrete Richtlinien zur Wahrung des Datenschutzes in speziellen Situationen.

Datenschutzrichtlinie All3DP GmbH

Begriffe und Abkürzungen

Die Begriffe definieren sich über die Begriffsdefinitionen der einzelnen geltenden Gesetze, insbesondere Artikel 4 DSGVO. Die wichtigsten Begriffe sind hier aufgeführt:

Begriff	Erklärung
personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“ oder „Betroffener“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, welche Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Verarbeitung	Jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Der Begriff der Verarbeitung wird den Begriffen Prozess oder Verfahren gleichgeschaltet.
Profiling	Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
Pseudonymisierung	Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.
Verantwortlicher	Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das

	Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.
Auftragsverarbeiter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Empfänger von Daten	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.
Dritter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

In der Richtlinie werden gegeben falls Abkürzungen verwendet, deren Bedeutung die folgende ist:

Abkürzung	Erklärung
BDSG-neu	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU). Die nationalen Datenschutzgesetze zur Umsetzung der Öffnungsklauseln aus der DSGVO.
DSB	Datenschutzbeauftragter
DSK	Datenschutzkoordinator
DSFA	Datenschutzfolgeabschätzung (nach Artikel 35 EU-DSGVO)
DSMS	Datenschutzmanagementsystem
EU-DSGVO oder DSGVO	Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)
EU-PrivacyVO oder PrivVO	E-Privacy-Verordnung (aktuell noch im Entwurf)
ISMS	Informationssicherheitsmanagementsystem (nach DIN ISO 27001)

Datenschutzrichtlinie All3DP GmbH

Organisation des Datenschutzes bei All3DP

Der Datenschutzbeauftragte von All3DP stellt ein fachlich weisungsunabhängiges Organ des Unternehmens dar und wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin. Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht deren Einhaltung. Seine genauen Aufgaben sind in Artikel 37 DSGVO geregelt.

Der Datenschutzbeauftragte wird von der Geschäftsleitung bestellt. Als Unterstützung seiner Tätigkeiten stehen ihm aus den Bereichen „Editorial“ und „Craftcloud“ sowie „IT“ und „Administration“ jeweils ein Ansprechpartner (Datenschutzkoordinator (DSK)) zur Verfügung.

Die Aufgabenbeschreibung der Datenschutzkoordinatoren sind im Rahmen der Unternehmensorganisation näher definiert und umfassen mindestens die zeitnahe Information zu Datenschutz-relevanten Themen und Risiken aus den jeweiligen Fachbereichen sowie die Mitwirkung an der Einhaltung des Datenschutzniveaus im Unternehmen.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit personenbezogener Datenverarbeitungen an den Datenschutzbeauftragten oder den für ihn zuständigen Datenschutzkoordinator wenden.

Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt und können direkt dem DSB gemeldet werden.

Anfragen von Aufsichtsbehörden und Betroffenen sind immer auch dem Datenschutzbeauftragten zur Kenntnis zu bringen.

Der Datenschutzbeauftragte kann wie folgt erreicht werden:

All3DP GmbH
c/o Datenschutzbeauftragter
Ridlerstr. 31A
D-80339 München

datenschutz@All3DP.de

Datenschutzrichtlinie All3DP GmbH

Grundsätze der Verarbeitung personenbezogener Daten

- **Rechtmäßigkeit und Verarbeitung nach Treu und Glauben**

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten dürfen nur auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden. Jede Verarbeitung muss auf ihre Rechtmäßigkeit durch den DSB geprüft werden.

- **Transparenz**

Personenbezogene Daten müssen in einer für den Betroffenen nachvollziehbaren Art und Weise verarbeitet werden. Betroffene müssen über die Art und Auswirkung der Datenverarbeitung angemessen und in klaren und verständlichen Worten informiert werden.

- **Zweckbindung**

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

- **Datenminimierung**

Die Verarbeitung personenbezogener Daten muss dem Zweck angemessen und auf das dafür notwendige Maß beschränkt sein.

- **Richtigkeit**

Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Es sind angemessene Maßnahmen zu treffen, dass unrichtige Daten unverzüglich gelöscht oder berichtigt werden können.

- **Speicherbegrenzung**

Personenbezogene Daten dürfen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Für alle Verarbeitungen sind deshalb Aufbewahrungs- oder Löschfristen zu definieren und einzuhalten.

- **Vertraulichkeit und Datensicherheit**

Personenbezogene Daten dürfen nur so verarbeitet werden, dass eine angemessene Sicherheit der personenbezogenen Daten gewährleistet ist. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch die Auswahl geeignete technische und organisatorische Maßnahmen mit ein.

Datenschutzrichtlinie All3DP GmbH

Zulässigkeit der Datenverarbeitung

Websitebesucher von All3DP und craftcloud3d.com

- **Datenverarbeitung für eine vertragliche Beziehung**

Personenbezogene Daten zu Nutzern der Website, Craftcloud-Kunden, Partnern und deren Angestellten oder Ansprechpartner dürfen nur zur Durchführung eines bestehenden oder angehenden Vertragsverhältnisses verarbeitet werden. Potentielle Interessenten dürfen zur Vertragsanbahnung nur unter den personenbezogenen Daten kontaktiert werden, die sie mitgeteilt haben.

Wendet sich der Betroffene mit einem Informationsanliegen (z.B. mit dem Wunsch nach Zusendung von Informationsmaterial zu einem Produkt oder Service) an das Unternehmen, so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

- **Datenverarbeitung zu Werbezwecken**

Kundenbindungs- oder Werbemaßnahmen bedürfen weiterer rechtlicher Voraussetzungen.

Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Werbung zu informieren. Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene soll über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert werden. Im Rahmen der Kommunikation mit dem Betroffenen sollte eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Werbezwecken eingeholt werden. Der Betroffene soll im Rahmen der Einwilligung zwischen den verfügbaren Kontaktkanälen wie Post, elektronische Post und Telefon wählen können.

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden.

- **Einwilligung in die Datenverarbeitung**

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene ausreichend und nachweislich informiert werden.

Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden.

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Der Betroffene muss über jede neue Art der Verarbeitung oder zu jedem einzelnen Zweck der Verarbeitung informiert werden und dieser einzeln zustimmen (Verkettungsverbot für Einwilligungen).

- **Datenverarbeitung aufgrund gesetzlicher Erlaubnis**

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

- **Datenverarbeitung aufgrund berechtigten Interesses**

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses von All3DP oder einem Dritten erforderlich ist. Berechtigte Interessen sind in der Regel rechtlicher (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftlicher Art (z.B. Vermeidung von Vertragsstörungen).

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung einzeln zu prüfen.

Die Gründe für die berechtigten Interessen sind zu dokumentieren und sowohl bei der Verarbeitungsübersicht als auch bei der Information zur jeweiligen Datenverarbeitung (Datenschutzerklärung im Internet oder auf Formularen) anzugeben.

- **Verarbeitung besonders schutzwürdiger Daten**

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten nach Artikel 9 DSGVO darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen.

Zu den besonders schutzwürdigen Daten zählen alle Angaben aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

- **Automatisierte Einzelentscheidungen**

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein. Dem Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden.

- **Nutzerdaten und Internet**

Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. Cookie-Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden. Ein personenbezogenes Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym,

so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out).

Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

Datenverarbeitung im Rahmen des Arbeitsverhältnisses

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind.

Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Konzerngesellschaften oder Partner erforderlich.

Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.

Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

- **Datenverarbeitung aufgrund gesetzlicher Erlaubnis**

Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

- **Kollektivregelungen für Datenverarbeitungen**

Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird. Kollektivregelungen sind Tarifverträge oder Vereinbarungen zwischen Arbeitgeber und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des Datenschutzrechts gestaltbar.

- **Einwilligung in die Datenverarbeitung**

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden.

- **Datenverarbeitung aufgrund berechtigten Interesses**

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung

eines berechtigten Interesses Unternehmens erforderlich ist. Berechtigte Interessen sind in der Regel rechtlicher (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlicher (z.B. Bewertung von Unternehmen) Art.

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind.

Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden.

Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen berücksichtigt werden.

- **Verarbeitung besonders schutzwürdiger Daten**

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden.

Zu den besonders schutzwürdigen Daten zählen alle Angaben aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein,

wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann.

Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen.

- **Automatisierte Entscheidungen**

Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (z.B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiter sein.

Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist. Dem betroffenen Mitarbeiter muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

- **Telekommunikation und Internet**

Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden.

Im Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das jeweils nationale geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen an den Übergängen in das All3DP-Netz implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets sowie der internen sozialen Netzwerke zeitlich befristet protokolliert werden.

Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien des Unternehmens erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Unternehmensregelungen, wie bspw. dem Code-of-Conduct.

Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb des Unternehmens oder an Empfänger innerhalb Unternehmens unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter dem vorrausgegangenen Abschnitt zu Websitenutzern, Craftcloud-Kunden, Partner und Mitarbeitern.

Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden. Im Falle einer Datenübermittlung an einen Empfänger außerhalb des Unternehmens in einem Drittstaat muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten.

Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt und dazu zwingend erforderlich ist.

Im Falle einer Datenübermittlung von Dritten an das Unternehmen muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

Werden personenbezogene Daten von einem All3DP Unternehmen mit Sitz im Europäischen Wirtschaftsraum an ein All3DP Unternehmen mit Sitz außerhalb des Europäischen Wirtschaftsraums (Drittstaat) übermittelt, so ist die datenimportierende Gesellschaft verpflichtet, bei allen Anfragen der für die datenexportierende Gesellschaft zuständigen Aufsichtsbehörde mit dieser zu kooperieren und die Feststellungen der Aufsichtsbehörde im Hinblick auf die übermittelten Daten zu beachten. Entsprechendes gilt für Datenübermittlungen durch All3DP Unternehmen aus anderen Staaten.

Auftragsverarbeitung und gemeinsame Verantwortung

Eine Auftragsverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. Hierbei greift Artikel 28 DSGVO. In diesen Fällen ist mit den externen Auftragnehmern eine Vereinbarung über eine Auftragsverarbeitung abzuschließen. Dabei behält All3DP die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung, deren Kontrolle sowie der Wahrnehmung der Rechte der von der Verarbeitung betroffenen Personen.

Sofern zwei oder mehrere verantwortliche Stellen die Mittel und die Zwecke einer Datenverarbeitung jedoch gemeinsam bestimmen, liegt eine Datenverarbeitung nach Artikel 26 DSGVO vor, welche dann ebenfalls einer besonderen vertraglichen Vereinbarung bedarf.

- **Auftragsverarbeitung nach Artikel 28 DSGVO**

Bei einer Auftragsverarbeitung nach Artikel 28 DSGVO darf der Auftragnehmer personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind deshalb die nachfolgenden Vorgaben einzuhalten, der beauftragende Fachbereich muss ihre Umsetzung sicherstellen:

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.
2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
3. Die vom DSB bereitgestellten Vertragsstandards müssen beachtet werden.
4. Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten

Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.

5. Bei einer grenzüberschreitenden Auftragsdatenverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau nachweist. Geeignete Instrumente können sein:
    a. Vereinbarung der EU-Standardvertragsklauseln zur Auftragsverarbeitung in Drittstaaten mit dem Auftragnehmer und möglichen Subunternehmern.
    b. Teilnahme des Auftragnehmers an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus (bspw. die PrivacyShield-Verfahren).
    c. Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutz-Aufsichtsbehörden.

- **Verarbeitung nach Artikel 26 DSGVO (Gemeinsam für die Verarbeitung Verantwortliche)**

Bei einer gemeinsamen Verarbeitung im Rahmen des Artikel 26 DSGVO legen die Vertragsparteien in einer schriftlichen Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Personen angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 DSGVO nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der EU oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind.

Die Vereinbarung muss beinhalten

1. die Angaben zu einer Anlaufstelle für die betroffenen Personen.
2. die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den betroffenen Personen.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sind sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen um die Rechte der betroffenen Personen zu schützen und den Anforderungen der DSGVO gerecht zu werden.

All3DP trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Dazu zählen bspw. u.a. die Verarbeitung nur von pseudonymisierten Daten, der Einsatz besonderer Authentifizierungsmaßnahmen (2-Faktor-Authentifizerung), die Vorbelegung mit datenschutzfreundlichen Grundeinstellungen in Checkboxen oder das Kennzeichnen von zu erhebenden Informationen als freiwillig.

Rechte des Betroffenen

Macht ein Betroffener von seinem Auskunftsrecht nach Artikel 15 DSGVO oder seinem Korrektur- oder Widerspruchsrecht nach Artikel 16 und 21 DSGVO Gebrauch, so erfolgt die zentrale Bearbeitung durch die Datenschutzkoordinatoren und den DSB. Die Auskünfte sind binnen einer Frist von 4 Wochen zu erteilen.

Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Personalverwaltung erfüllt.

Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können. Welcher Standard diesen Anforderungen genügt, ist im Vorfeld einvernehmlich durch den DSB und die IT festzulegen und sind in einer Prozessbeschreibung zu definieren. Dabei müssen nur solche Daten bereitgestellt werden, welche vom Betroffenen auch an All3DP übermittelt wurden.

Auskünfte sind generell schriftlich an die ALL3DP bekannte Adresse zu erteilen. Zur Sicherstellung der Identität des Auskunft-Suchenden kann bei unbekannter Adresse oder Zweifeln an der Richtigkeit der Angaben das ID-Check-Verfahren eingesetzt werden.

Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen der Vertraulichkeit. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt.

Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten. Dieses Prinzip ist sowohl durch die eigene IT als auch in Auftragsverarbeitungs- oder Software-Entwicklungsprozessen sicherzustellen.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

Vorgesetze müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

All3DP stellt hierzu besondere Formulare zur Verfügung. Abhängig von der Rolle im Unternehmen hat jeder Mitarbeiter, aber auch externe Dienstleister entsprechende Verpflichtungserklärungen u.a. zur Wahrung der Vertraulichkeit von personenbezogenen Daten (Datengeheimnis) zu unterzeichnen.

Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt.

Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren.

Der verantwortliche Unternehmensbereich kann dazu insbesondere den Informationssicherheitsbeauftragten und den Datenschutzkoordinator zu Rate ziehen. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des unternehmensweiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

Datenschutzfolgeabschätzung (DSFA)

Hat eine Form der Verarbeitung personenbezogener Daten, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchgeführt werden.

Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Die Verantwortung für die Durchführung der DSFA hat der DSB, die zuständigen Fachbereiche und deren DSK sowie die IT. Die DSFA ist entsprechend zu dokumentieren.

Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem DSB, den Datenschutzkoordinatoren und weiteren, mit Auditrechten ausgestatteten Unternehmensbereichen oder beauftragten externen Prüfern.

Die Ergebnisse der Datenschutzkontrollen sind dem DSB mitzuteilen. Die Geschäftsleitung ist im Rahmen der jeweiligen Berichtspflichten über wesentliche Ergebnisse zu informieren. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt.

Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

Die zuständige Aufsichtsbehörde von All3DP ist aktuell:

Bayerisches Landesamt für Datenschutzaufsicht

Hausanschrift: Promenade 18, 91522 Ansbach, Deutschland
Postanschrift: Postfach 1349, 91504 Ansbach, Deutschland
Telefon: +49 (0) 981 180093-0, Telefax: +49 (0) 981 180093-800, E-Mail: poststelle@lda.bayern.de

Datenschutzvorfälle

Jeder Mitarbeiter soll seinem jeweiligen Vorgesetzten, seinem Datenschutzkoordinator oder dem DSB unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten melden.

Die für die Funktion oder die Einheit verantwortliche Führungskraft ist verpflichtet, den zuständigen Datenschutzkoordinator oder den DSB umgehend über Datenschutzvorfälle zu unterrichten.

In Fällen von (oder auch nur bei Bekanntwerden von)

a) unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
b) unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder
c) bei Verlust personenbezogener Daten

sind die im Unternehmen vorgesehenen Meldungen unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

Verantwortlichkeiten und Sanktionen

Die Geschäftsführung des Unternehmens ist verantwortlich für die Datenverarbeitung im Unternehmen. Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. nationale Meldepflichten). Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen.

Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter. Bei Datenschutzkontrollen durch Behörden ist der DSB umgehend zu informieren.

Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen die Datenschutzkoordinatoren und/oder den DSB rechtzeitig über neue Verarbeitungen

personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der DSB schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten. Die Führungskräfte müssen sicherstellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen.

Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.