RISIKEN IN DER DATENVERARBEITUNG

PROZESSE / SCHRITTE	PERSONEN-BEZOGENE DATEN	HOHE RISIKEN
Personal-management	Aufnahme von Mitarbeiterdaten bei der Einstellung und kontinuierliche Ergänzung	· Verlust · Diebstahl · Nicht termingerechtes Löschen · Unrechtmäßige Erhebung
Dienstleister-management	Aufnahme von personenbezogenen Daten der Dienstleister und Verarbeitung von Daten im Rahmen der Zusammenarbeit	· Verlust · Diebstahl · Fehlerhafte Daten
Kunden-management	Mindestens Aufnahme von Kontakt- und Rechnungsdaten und Speicherung in einem CRM-System	· Verlust · Fehlerhafte Daten · Diebstahl · Unrechtmäßige Erhebung
Auftrags-erfüllung		
Auftragsauf-nahme	Übermittlung der Kundendaten und der Daten für das gewünschte Produkt	· Unrechtmäßige Erhebung · Fehlerhafte Daten · Diebstahl
Daten-aufbereitung	Umwandlung der Produktdaten in die entsprechenden Formate	· Diebstahl
Fertigung	Additive Herstellung des Produkts und anschließende Nachbereitung	· Diebstahl
Auslieferung	Auslieferung der Ware und der Rechnung unter Angabe von Name und Anschrift von Aussteller und Empfänger, Rechnungsnummer und Preis	· Diebstahl · Verlust
Zweck-erfüllung	Löschung oder Sperrung der personenbezogenen Daten nach Ablauf der Zweckerfüllung	· Nicht termingerechtes Löschen

WARUM DATENSCHUTZ?

Datenschutz soll Unternehmen nicht hemmen, sondern ihnen bei der Gestaltung ihrer Geschäftsbeziehungen behilflich sein, denn er ist ein wesentlicher Baustein gelungener digitaler Transformation.

Aus folgenden Gründen ist Datenschutz in KMU besonders relevant:

- Schutz vor Internetkriminalität
- Datenschutz als Wettbewerbsvorteil
- Verantwortung gegenüber ihren Kunden und deren Daten
- Respekt vor dem Recht auf Selbstbestimmung
- Prozessoptimierung durch neue Lösungen
- Vertrauen der Mitarbeiter und gutes Betriebsklima
- Bei Nichteinhaltung drohen hohe Geldstrafen

HESSEN Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung

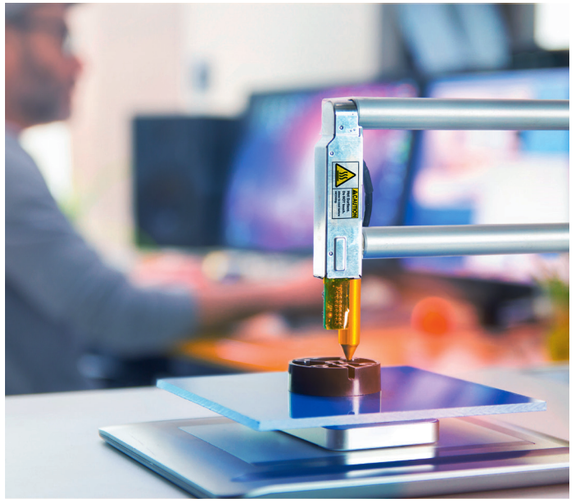
Projektträger:

HESSEN TRADE & INVEST

Wirtschaftsförderer für Hessen

Hessen Trade & Invest GmbH
Konradinerallee 9
65189 Wiesbaden
Telefon: +49 611 9501785
E-Mail: info@technologieland-hessen.de
www.technologieland-hessen.de

HESSEN TECHNOLOGIELAND HESSEN



DATENSCHUTZ FÜR UNTERNEHMEN MIT ADDITIVER FERTIGUNG

Hinweise und Handlungsempfehlungen

www.technologieland-hessen.de

VRNTZT. ZKNFT. GSTLTN.

Die Additive Fertigung lebt von der Datenverarbeitung auf vielen verschiedenen Ebenen: Beim Design und in der Entwicklung, im Fertigungsprozess, beim Austausch von Daten mit Auftraggebern bis hin zur Abwicklung von Kundenbestellungen.

Veränderte rechtliche Rahmenbedingungen für Unternehmen der additiven Fertigung liegen seit Inkrafttreten der Europäischen Datenschutz-Grundverordnung (DSGVO) vor. Entsprechende Maßnahmen und Anpassungen sind notwendig, um den neuen Anforderungen gerecht zu werden und hohe Bußgelder zu vermeiden.

DATENSCHUTZ UND DATENSCHUTZRECHT

Datenschutz baut auf dem Recht auf, nach dem jeder Mensch selbst entscheiden kann, wem, wann und welche seiner persönlichen Daten er zugänglich machen will. Das Datenschutzrecht regelt entsprechend die Verarbeitung personenbezogener Daten. Soweit keine personenbezogenen Daten betroffen sind, findet die DSGVO keine Anwendung.

PERSONENBEZOGENE DATEN IN DER ADDITIVEN FERTIGUNG

Die Tragweite der datenschutzrechtlichen Bestimmungen hängt maßgeblich davon ab, wie und in welchem Umfang personenbezogene Daten verarbeitet werden. Dies unterscheidet sich vor allem nach branchen- und fertigungsspezifischen Eigenheiten:

- Neben dem Personal- und Kundenmanagement können in der Additiven Fertigung (AF) auch personenbezogene Daten in der individuellen Produktentwicklung sowie der datengetriebenen Produktion anfallen.
- In der Medizintechnik sowie Lifestyle- und Foodindustrie werden personenbezogene Daten auch im Fertigungsprozess verarbeitet, während sie in der Automobil-, Werkzeug- und Maschinenbauindustrie eher selten sind.
- Bei Geschäftsbeziehungen zwischen Unternehmen (B2B), fallen in der Regel weniger personenbezogene Daten an als im Verkehr mit Privatpersonen (B2C).

➔ Jedes Unternehmen muss seine individuellen Strukturen und Prozesse analysieren, um die vom Datenschutzrecht betroffenen Daten zu identifizieren.

HANDLUNGSEMPFEHLUNGEN

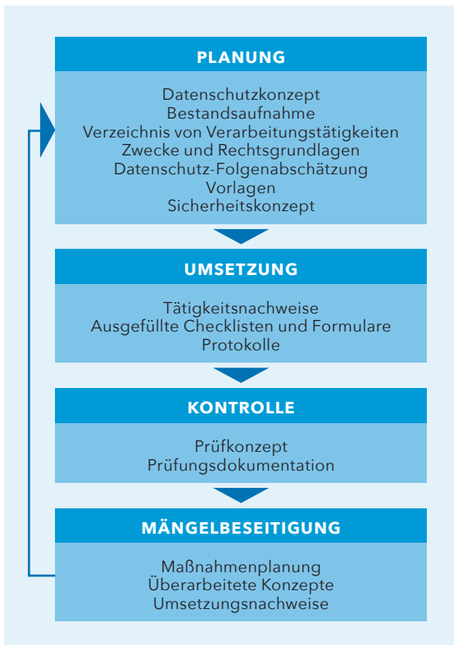
Handlungsempfehlungen für alle Unternehmen

Datenschutz im Unternehmen richtig planen und organisieren

- ➔ Anwendungsbereich identifizieren: Bestandsaufnahme personenbezogener Daten und Prozesse der Verarbeitung durchführen
- ➔ Datenschutzmanagement etablieren: Datenschutzkonzept erstellen, Datenschutzmaßnahmen planen und Datenschutzprozesse einführen
- ➔ Risiken bei der Datenverarbeitung abschätzen: Datenschutz-Folgenabschätzung (DFSA) durchführen

Pflichten nachkommen und Rechte gewähren

- ➔ Dokumentationspflicht erfüllen: Verzeichnis von Verarbeitungstätigkeiten einführen bzw. aktualisieren



Mögliche Elemente der Datenschutzdokumentation

- ➔ Betroffenenrechte einhalten: Datenschutzerklärungen und -informationen anpassen, Prozess für Anfragen betroffener Personen einführen
- ➔ Meldeprozess für Datenpannen etablieren, um der Meldepflicht nachzukommen

Risiken bei der Datenverarbeitung entgegenwirken

- ➔ Technische und organisatorische Maßnahmen planen und umsetzen
- ➔ Verträge mit Dienstleistern anpassen, um Sicherheit auch bei der Auftragsdatenverarbeitung zu garantieren

Checkliste

MASSNAHMEN	EINZELSCHRITTE	ZIEL DER MASSNAHME
Datenschutzfolgenabschätzung (DSFA)	✓ Team, Prüfplanung und betroffene Personen definieren ✓ Notwendigkeit der Verarbeitung personenbezogener Daten bewerten ✓ Risikobewertung durchführen ✓ Abhilfemaßnahmen auswählen, umsetzen und dokumentieren	· Systematische Risikoeindämmung · Verständnis der eigenen Prozesse bei der Datenverarbeitung herstellen · Pflichten erfüllen
Auftragsverarbeitung	✓ Verträge in beide Richtungen prüfen ✓ Als Auftragnehmer: Datenschutz vertraglich zusichern ✓ Als Auftraggeber: Datenschutz garantieren lassen ✓ Als Auftragsverarbeiter: Zum Datenschutz verpflichten	· Rechtssichere Beziehungen zu Dienstleistern schaffen · Vertrauensbasis sichern
Technische und organisatorische Maßnahmen (TOM)	✓ Technische und physische IT-Sicherheit ✓ Mitarbeiterschulungen ✓ Meldeprozess etablieren ✓ Zertifizierungen (z. B. zur IT-Sicherheit)	· Eigen- und Fremdschutz absichern · Etablierte Frühwarnsysteme

Spezifische Handlungsempfehlungen für die additive Fertigung

Klassifikation der Daten

- ➔ Daten nach Schutzstufen kategorisieren zur Priorisierung und angemessenen Gestaltung der technischen und organisatorischen Maßnahmen (TOM)

Verschlüsselung und Pseudonymisierung

- ➔ Fertigungsaufträge konsequent verschlüsseln und pseudonymisieren (z. B. mithilfe von Zahlen und Nummern), um einen Personenbezug auszuschließen

Umgang mit Auftragsverarbeitern

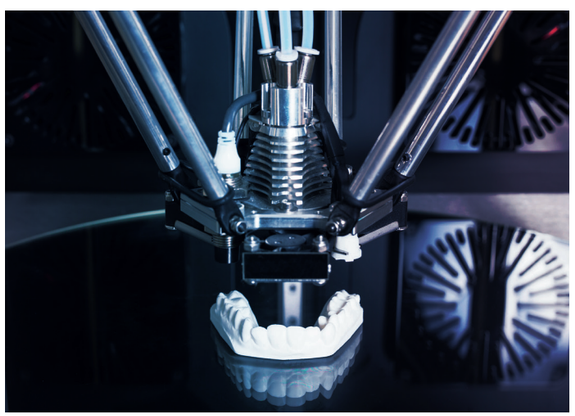
- ➔ Dienstleister auf Einhaltung des Datenschutzrechts prüfen (z. B. durch Zertifizierungen) und entsprechende Bestimmungen vertraglich festlegen

Löschen von Daten

- ➔ Prozesse zur Löschung von Konstruktionsdaten auf personenbezogene Daten ausweiten, sobald der Verarbeitungszweck entfallen ist

Informationspflicht

- ➔ Im Rahmen der Informationspflicht vor der Fertigung darauf hinweisen, dass auch die Konstruktionsdaten in der Verarbeitung möglicherweise einen Personenbezug erlauben



WICHTIGE BEGRIFFLICHKEITEN

Europäische Datenschutzgrundverordnung (DSGVO)

Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden

Bundesdatenschutzgesetz (BDSG)

Die DSGVO bedeutet gleichzeitig eine Anpassung des nationalen Rechts in Form einer Neufassung des BDSG, das parallel anzuwenden ist

Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

Besonders sensible personenbezogene Daten

Daten zur rassischen und ethnischen Herkunft, politischen Meinung, religiösen oder weltanschaulichen Überzeugung, Gewerkschaftszugehörigkeit, genetische und biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung

Datenverarbeitung

Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten

Datenschutz-Folgenabschätzung (DSFA)

Prozess zur Abschätzung der Folgen vor Beginn von einzelnen, geplanten Datenverarbeitungsvorgängen

Technische und organisatorische Maßnahmen (TOM)

Gewährleistung eines der Datenverarbeitung angemessenen Schutzniveaus, das im weitesten Sinne physisch, in Soft- und Hardware sowie durch Handlungsanweisung oder Verfahrens- und Vorgehensweisen umgesetzt wird