antares

EU-DSGVO-Checkliste

[5 Top-Themen der EU-DSGVO

Im Jahr 2018 trat die neue EU-Datenschutz-Grundverordnung (EU-DSGVO) in Kraft. Dies hatte weitreichende Konsequenzen für Unternehmen, die personenbezogene Daten verarbeiten. Alle darauf bezogenen Strukturen und Prozesse mussten entsprechend der erhöhten Anforderungen angepasst werden.

Neben Neuerungen zum Datenschutz hat sich auch die Unternehmenshaftung erweitert. Bei einem Verstoß drohen empfindlich hohe Bußgelder, die im Extremfall bis zu 4% des Jahresumsatzes ausmachen können.

Diese Checkliste soll eine Zusammenfassung der Kernpunkte dieser EU-DSGVO geben.*

[Datenschutzmanagement und Informationssicherheit

Wir helfen Ihnen bei der Integration einer Datenschutzmanagement-Software - mit antares RiMIS® ISMS und antares RiMIS® DSMS. Wir unterstützen Sie bei der Zertifizierung nach ISO 27001 und auf Basis vom IT-Grundschutz. Durch die Zertifizierung zeigt Ihr Unternehmen, dass geeignete Maßnahmen zur Absicherung der IT-Systeme umgesetzt wurden.

Durch die Integration der Anforderungen aus der EU-DSGVO in Ihr Informationssicherheits-Managementsystem zeigen Sie Ihren Kunden und Partnern, dass alle erforderlichen Maßnahmen zum Datenschutz getroffen wurden. Ein effizientes DSMS unterstützt Sie nicht nur dabei, Datenschutz- und Informationssicherheits-Risiken frühzeitig zu erkennen und nachhaltig zu minimieren, sondern auch Ihre Unternehmenswerte abzusichern. Steuern Sie Risiken gezielt und behalten Sie die Kontrolle über alle Gegenmaßnahmen jederzeit im Auge!

[Datenschutzprinzipien

Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, solange die betroffene Person nicht eingewilligt hat oder es durch ein Gesetz ausdrücklich erlaubt ist. Dabei müssen die Datenschutzprinzipien zu jeder Zeit eingehalten werden, denn der Verstoß dagegen kann hohe Bußgelder zur Folge haben. Dies ist z. B. der Fall, wenn zwar eine Einwilligung des Betroffenen vorliegt, aber überflüssige Daten erhoben werden und es dadurch dem Prinzip der Datensparsamkeit widerspricht.

Rechtmäßigkeit

Jede Datenverarbeitung, die nicht durch eine Einwilligung des Betroffenen abgedeckt ist, bedarf einer gesetzlichen Erlaubnis. Soweit kein Erlaubnistatbestand vorliegt, dürfen die Daten nicht verarbeitet werden.

Beispiel: Für das Versenden von Newslettern gibt es keine pauschale gesetzliche Erlaubnis. Die Einwilligung ist von jedem Empfänger vorab gesondert einzuholen.

Datensparsamkeit

Eine Datenverarbeitung muss dem Zweck angemessen sowie auf das notwendige Maß beschränkt sein.

Beispiel: Bei einer Bestellung darf keine Telefonnummer erhoben werden, wenn sie für die Bestellabwicklung nicht notwendig ist.

Zweckbindung

Die Datenverarbeitung darf nur zu vorher festgelegten, eindeutigen und legitimen Zwecken erfolgen. Im Fall einer Zweckerreichung müssen die Daten unverzüglich gelöscht werden.

Beispiel: Im Anmeldeformular für einen Newsletter muss der Zweck (z. B. die Zusendung von Produktempfehlungen oder Tipps) angegeben werden.

Datensicherheit

Bei der Verarbeitung von Daten müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um den Schutz vor Datenmissbrauch zu gewährleisten.

Beispiel: Wer mit sensiblen Daten (z. B. Krankenakten oder Passwörter) arbeitet, muss gewährleisten, dass unberechtigte Personen keinen Zugriff darauf haben.

Transparenz

Die betroffene Person muss die Datenverarbeitung nachvollziehen können. Darunter fällt z.B., welche Daten in Bezug auf ihre Person erhoben werden.

Beispiel: Wer Daten ohne Wissen eines Websitebesuchers erhebt, muss mindestens in der Datenschutzerklärung darüber aufklären.

[5 Top-Themen der EU-DSGVO

1. Anwendungsbereich der EU-DSGVO (Art. 2-3)

Die Regelungen der EU-DSGVO gelten für alle Unternehmen, die in einem EU-Mitgliedsstaat niedergelassen sind. Dabei spielt es keine Rolle, ob die Datenverarbeitung in- oder außerhalb der EU stattfindet.

Außerhalb der EU finden die Regelungen Anwendung, wenn die Datenverarbeitung in Zusammenhang mit dem Anbieten von Waren/Dienstleistungen oder dem Verfolgen des Nutzerverhaltens von EU-Bürgern besteht.
Genauso sind Unternehmen betroffen, die ihre Datenverarbeitung in Staaten außerhalb der EU auslagern (z. B. Server in USA anmieten).

Was fällt unter personenbezogene Daten?
Personenbezogene Daten sind sämtliche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Dazu gehören nicht nur Adressdaten oder die E-Mail-Adresse, sondern explizit auch Online-Daten, wie beispielsweise die IP-Adresse, Cookies oder Informationen zum Gerät einer Person.

„Identifizierbar" ist eine Person zudem künftig auch dann, wenn ihre Daten zwar anonymisiert wurden, aber mit weiteren Informationen zusammengeführt zurückverfolgbar werden.

2. Einwilligung zur Verarbeitung und Nutzung personenbezogener Daten (Art. 6)

Eine Verarbeitung von personenbezogenen Daten ist neben einer ausdrücklichen Erlaubnis des Betroffenen ebenfalls zulässig, wenn gesetzlich vorgeschriebene Erlaubnistatbestände Anwendung finden.

Die Erlaubnistatbestände nach der EU-DSGVO sind:

- Es liegt die Einwilligung der betroffenen Person vor;
- Es gibt ein berechtigtes Interesse an der Datenverarbeitung und schutzwürdige Interessen des Betroffenen stehen dem nicht entgegen;
- Die Datenverarbeitung ist erforderlich
  - zur Erfüllung eines Vertrags;
  - für vorvertragliche Maßnahmen auf eine Anfrage hin;
  - zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen.

Was muss beim Einholen einer Einwilligungserklärung berücksichtigt werden?

Einwilligungen können schriftlich, elektronisch oder mündlich erfolgen und müssen vom erhebenden Unternehmen im Zweifelsfall nachgewiesen werden. An dieser Stelle sollte der Betroffene zudem neben einem Hinweis auf sein Widerrufsrecht die Informationen erhalten, wer seine Daten verarbeitet und zu welchem Zweck.

Weitere Vorgaben können sich für spezielle Situationen ergeben. Beispielsweise sollte es bei der Anmeldung zu einem Newsletter keine vorangeklickten Checkboxen geben, da eine Einwilligung ausdrücklich und damit aktiv gegeben werden muss. Zudem sollte bei Anmeldungen mit dem Double-Opt-in-Verfahren gearbeitet werden.

3. Auftragsverarbeitung (Art. 28, 32)

Jegliche Art von Auftragsverarbeitung fällt künftig in den Bereich der EU-DSGVO. Ein Auftragsverarbeiter (=Auftragsnehmer) wird definiert als eine Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen (=Auftraggeber) verarbeitet.

Die Auftragsverarbeiter folgen dabei den Anweisungen ihrer Auftraggeber. Jedoch müssen sie dabei garantieren, dass sie die Vorgaben der EU-DSGVO einhalten.

Beispiel: Anbieter von Cloud-Diensten müssen garantieren, dass geeignete technische und organisatorische Maßnahmen vorliegen, um den Anforderungen des Datenschutzes und der Datensicherheit zu entsprechen. Hierzu zählen z. B. Zertifikate wie etwa die Norm ISO/IEC 27001.

Weitere Beispiele aus der Praxis:
- Lohnbuchhaltung in der Cloud
- Nutzung einer CRM-Anwendung in der Cloud
- Versenden von Newslettern über einen Cloud-Anbieter

Bislang war der Auftragnehmer an die Weisungen des Auftraggebers gebunden und der Auftraggeber blieb dadurch voll verantwortlich. Die neue EU-DSGVO verpflichtet nun auch den Auftragnehmer, wodurch dieser bei einem Verstoß ebenfalls haftet.

Folgende Pflichten haben Auftragsverarbeiter:
- Dokumentationspflichten (Verfahrensverzeichnis)
- Umsetzung technischer und organisatorischer Maßnahmen, um die Datensicherheit zu gewährleisten
- Bestellung eines Datenschutzbeauftragten
- Meldepflichten bei Datenpannen

Diese Grundsätze gelten uneingeschränkt nur dann, wenn Auftraggeber und Auftragnehmer innerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) ansässig sind und die Datenverarbeitung in diesem Bereich stattfindet. Hat eine der genannten Stellen ihren Sitz nicht in der EU und verlassen die Daten im Zuge des Auftrags den Bereich der EU/des EWR, dann sind die Regelungen der EU-DSGVO zum Drittstaatentransfer zu beachten.

Unser Tipp: Gehen Sie auf Nummer sicher! Lassen Sie sich die EU-DSGVO-Konformität Ihrer Dienstleister bestätigen oder greifen Sie auf bereits zertifizierte Anbieter zurück.

Wie beauftragen Sie den Auftragsverarbeiter?

Nach der EU-DSGVO ist es nicht mehr erforderlich, einen schriftlichen Vertrag zur Auftragsdatenverarbeitung zu schließen. Es ist ausreichend, die gegenseitigen Rechte und Pflichten in den jeweiligen Auftrag aufzunehmen.

4. Verzeichnis der Verarbeitungstätigkeiten (Art. 30)

Die EU-DSGVO sieht vor, dass Unternehmen ein Verzeichnis über alle Verarbeitungstätigkeiten führen müssen.

Eine Einschränkung besteht für Unternehmen mit weniger als 250 Mitarbeitern, die nur in den folgenden Fällen kein Verzeichnis führen müssen:
- Die vorgenommene Verarbeitung birgt kein Risiko für die Rechte und Freiheiten der Betroffenen.
- Die Datenverarbeitung erfolgt nur gelegentlich.
- Es werden keine sensitiven Daten verwendet.

Ein Verzeichnis der Verarbeitungstätigkeiten sollte folgende Angaben beinhalten:

- Name, Kontaktdaten, Vertreter, Datenschutzbeauftragter
- Zweck der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die Daten offengelegt wurden oder werden (auch im EU-Ausland)
- Fristen für die Löschung der Datenkategorien
- Beschreibung der technischen und organisatorischen Maßnahmen

Unser Tipp: Bestimmen Sie schnellstmöglich ein Team zur Erstellung eines Verfahrensverzeichnisses. Dabei können Schwachstellen im Prozess der Datenverarbeitung des eigenen Unternehmens aufgedeckt und behoben werden.

5. Bestellung eines Datenschutzbeauftragten (Art. 37-39)

Unternehmen mit mindestens 10 Mitarbeitern, die personenbezogene Daten automatisiert verarbeiten, müssen einen Datenschutzbeauftragten bestellen. In Unternehmen mit weniger als 9 Mitarbeitern kann die Geschäftsführung die Aufgaben des Datenschutzbeauftragten übernehmen.

Die Ausnahme gilt bei extrem sensiblen Daten wie Herkunft, Gesundheit oder politische Einstellung einer Person. In diesen Fällen müssen auch kleine Betriebe einen Datenschutzbeauftragten bestellen.

Welche Aufgaben hat ein Datenschutzbeauftragter?

Die Kerntätigkeit liegt darin, die Verarbeitung von personenbezogenen Daten regelmäßig und systematisch zu beobachten. Die daraus resultierenden Empfehlungen sollten von der Geschäftsführung umgesetzt werden.

Als Hilfestellung dient dabei diese Checkliste*: www.lda.bayern.de/media/dsgvo_fragebogen.pdf.

Beispiel für ein Verzeichnis der Verarbeitungstätigkeiten:

Nr.	Gemeinsam Verantwortliche	Zweck	Betroffenengruppen	Datenkategorien	Empfänger	Übermittlung an Drittstaaten	Löschfrist	Technische & organisatorische Maßnahmen (TOM)
01		Marketing & Vertrieb	a. Aktive und ehemalige Kunden b. Interessenten c. Websitebesucher	Zu a & b: Kontakt- und Listendaten, Produktinteressenten, Kommunikationshistorie, Bonitätsinformationen Zu a: Stamm- und Vertragsdaten der Kaufhistorie Zu c: Pseudonymisierte Profile gem. § 15 TMG (Tele-Medien-Gesetz)	Marketing, Vertrieb, Externe Dienstleister	Übermittlung pseudonymisierter Trackingdaten an US-Dienstleister	Zu a & b: Bei Widerruf durch Betroffenen oder 2 Jahre nach Beendigung der Kundenbeziehung Zu c: Nach 6 Monaten durch Aggregation	

* Diese Datei wird bereitgestellt vom Bayerischen Landesamt für Datenschutzaufsicht.

[Wir stellen uns vor

Das machen wir

Wir sind ein mittelständisches, unabhängiges und auf professionelle Software spezialisiertes Unternehmen. Seit unserer Gründung im Jahr 1994 entwickeln und vermarkten wir strategische Informationssysteme.

Langjährige Expertise in den Themen Analyse, Planung und Unternehmenssteuerung sowie Governance, Risk und Compliance sind Garanten für den Auf- und Ausbau der fortschrittlichen antares-Softwarelösungen.

Das sind wir

Modernste Technologie, Innovation und anwenderoptimierte Lösungen prägen unsere Produkte. Leidenschaft, Zuverlässigkeit und Professionalität sind die Leitlinien im Umgang mit unseren Kunden und Partnern. Der kompetente und zuverlässige Support steht bei uns an erster Stelle. Um das zu gewährleisten, arbeiten wir konsequent an der Weiterentwicklung unserer etablierten Softwarelösungen, übernehmen das professionelle Projektmanagement und bieten darüber hinaus umfassende Dienstleistungen - von Schulungen und Webinaren bis hin zu Coachings.

Das bieten wir

Wir zählen mittlerweile mehr als 300 Unternehmen aller Branchen und Größenordnungen zu unseren Kunden, darunter namhafte Unternehmen aus den Bereichen Industrie, Handel und Dienstleistung. Sie alle profitieren von einem erfahrenen BI-Unternehmen mit flachen Hierarchien, professioneller Partnerschaftlichkeit und Kundennähe.

Das ist unser Ziel

Unser Ziel ist es, unseren Kunden stets eine sichere, benutzerfreundliche Informationsbasis zu verschaffen, damit bewusste und sichere Entscheidungen getroffen werden können.

antares

[Software für sichere Entscheidungen

[Software für sichere Entscheidungen

antares Informations-Systeme GmbH
Stuttgarter Str. 99
D-73312 Geislingen

Tel. +49 7331 3076-0

www.antares-is.de
info@antares-is.de