PKF WMS

Checkliste DSGVO

WAS SIND PERSONENBEZOGENE DATEN

- Personenbezogene Daten sind nach Artikel 4 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

- Juristische Personen (Unternehmen, GmbHs, öffentliche Stellen oder Einrichtungen) sind somit nicht durch die Vorschriften der DSGVO geschützt. Das gilt ebenso für die Daten Verstorbener.

- Zu den geschützten Informationen gehören z.B.

  - Namen
  - Adressen
  - Geburtsdaten
  - Bankverbindungen
  - Telefonnummern
  - E-Mail-Adressen

- Es reicht aus, wenn sich eine Person indirekt identifizieren lässt, etwa durch Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, zu Standortdaten (Mobilfunk, Navigationsgerät) oder zu einer Online-Kennung (IP-Adressen, Cookies, Funkfrequenzkennzeichnungen).

- Sind personenbezogene Daten vollständig anonymisiert und ist keine Identifizierung mehr möglich, so unterliegen diese Daten nicht mehr den Vorschriften der Datenschutz-Grundverordnung.

DATENSCHUTZ IST CHEFSACHE

Haben Sie sich als Geschäftsleitung schon mit den neuen Anforderungen der DSGVO und des BDSG (neu) befasst? Kennen Sie insbesondere die neuen Regelungen:

- zu den Rechten der Betroffenen wie Auskunft oder Datenübertragbarkeit?
- zu den Informationspflichten gegenüber den Betroffenen, deren Daten Sie verarbeiten?
- zur Rechenschaftspflicht über die Einhaltung der Grundsätze der Datenverarbeitung?
- zur technischen und organisatorischen Sicherheit der Datenverarbeitung?
- zur Datenschutz-Folgenabschätzung?
- zur Meldung von Datenschutzverstößen?

Die Geschäftsführung ist gegenüber der Aufsichtsbehörde zur Rechenschaft verpflichtet!

Im Falle eines Datenschutzverstoßes kann die Geschäftsführung persönlich haftbar gemacht werden.

HABEN BZW. BRAUCHEN SIE EINEN DATEN-SCHUTZBEAUFTRAGTEN

Sind in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung beschäftigt?

Werden besondere Kategorien personenbezogene Daten verarbeitet, wie z. B. über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche

Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten oder Daten zum Sexualleben einer Person?

Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet?

Nutzen Sie eine Videoüberwachung?

Falls „ja“ müssen Sie

- einen Datenschutzbeauftragten bestellen
- dessen Kontaktdaten auf Ihrer Webseite veröffentlichen
- diese der zuständigen Aufsichtsbehörde mitteilen

BESTANDSAUFNAHME

Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, erfasst?

Besteht für alle bereits ein „Verfahrensverzeichnis“?

Wurde schon mit der Überführung in das Verzeichnis von Verarbeitungstätigkeiten begonnen?

Denken Sie hierbei insbesondere an die:
- Verarbeitung von Kundendaten
- Verarbeitung von Beschäftigtendaten
- Verarbeitung von Daten von Kindern
- Verarbeitung von Daten für Dritte als Auftragsverarbeiter

Wird dieses Verzeichnis regelmäßig aktualisiert?

Wer ist hierfür in Ihrem Unternehmen zuständig?

Das Verzeichnis von Verarbeitungstätigkeiten ist das „Einfallstor“ der Aufsichtsbehörde!

RECHTMÄßIGKEIT DER VERARBEITUNG

Auch nach neuem Recht benötigen Sie für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage. Dies kann eine gesetzliche Regelung, eine Einwilligung der Betroffenen oder eine Betriebsvereinbarung sein.

- Haben Sie für alle Verarbeitungen eine Rechtsgrundlage “lokalisiert“?
- Haben Sie die Rechtsgrundlage dokumen tiert?
- Sind Anpassungen z.B. an die Informationspflichten für Betroffene erforderlich?
- Haben Sie Ihre Muster für Einwilligungserklärungen für Kunden, Interessenten usw. an die Anforderungen der DSGVO angepasst (insbesondere: erweiterte Informationspflichten, auch zur jederzeitigen Widerrufbarkeit der Einwilligung)?
- Sind Ihre alten Datenbestände auch ab dem 25.5.2018 nutzbar, weil z.B. eine rechtskonforme Einwilligung vorliegt?

STELLEN SIE DIE DATENSCHUTZ-COMPLIANCE SICHER

Haben Sie alle Prozesse erfasst?

Können Sie die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen? D.h. haben Sie es „schwarz auf weiß“?

Wer ist im Unternehmen für was im Datenschutz zuständig?

Gibt es Arbeitsanweisungen/Richtlinien zur Bearbeitung von Anfragen von Betroffenen?

Haben Sie einen Steuerungsprozess für die Dokumente?

Haben Sie die Archivierung geregelt?

PKF WMS

SIND IHRE MITARBEITER VERPFLICHTET?

Welche Mitarbeiter verarbeiten personenbezogene Daten?

Existiert für diese Mitarbeiter eine neue „Verpflichtungserklärung“?

Wer ist für die Einholung verantwortlich?

Wer für die Aufbewahrung?

Wie läuft der Prozess bei Neueinstellungen?

SCHULEN SIE IHRE MITARBEITER

Wie müssen Ihre Mitarbeiter ab dem 25.05.2018 reagieren wenn Betroffene ihr Recht auf

- Information
- Löschung
- Berichtigung

usw. wahrnehmen?

Welche personenbezogenen Daten dürfen noch erfasst werden?

Wo werden diese Daten gespeichert (Warenwirtschaft, Outlook, Fileserver, Cloud, usw.)?

Wie bleiben personenbezogene Daten sicher, wodurch entstehen Datenlecks?

PRÜFEN SIE IHRE AUßENWIRKUNG

Entspricht die Datenschutzerklärung den Anforderungen der DSGVO?

Prüfen Sie Ihre AGBs ob diese Klauseln zum DS-Recht enthalten.

Gibt es auf Ihrer Webseite Kontaktformulare oder Login-Bereiche und sind diese Webseiten ausreichend verschlüsselt?

Nutzen Sie Google Analytics/Piwik oder ähnliches und weisen Sie entsprechend darauf hin?

Nutzen Sie Cookies?

Sind die Anforderungen an Einwilligungen z.B. für Newsletter eingehalten?

VERTRÄGE PRÜFEN

Wer bekommt von Ihnen Geld für die Verarbeitung personenbezogener Daten?

Wo sind die (Leistungs-)Verträge?

Gibt es dazu auch immer einen Vertrag über die Auftragsverarbeitung?

Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern, d.h. mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, an die neuen Regelungen (Art. 26 – 28 DS-GVO) angepasst? Bsp.: Call-Center, Lohndienstleister, Softwareanbieter, Aktenentsorger

Dokumentieren Sie Anweisungen, die Sie Ihren Auftragsverarbeitern geben?

Bestehen für alle Verarbeitungen, bei denen eine Übermittlung personenbezogener Daten in ein Drittland möglich ist, entsprechende zusätzliche Garantien / Vereinbarungen?

- EU-Standardvertragsklauseln
- Binding Corporate Rules
- Privacy Shield (nur für die USA)

DATENSCHUTZ-FOLGENABSCHÄTZUNG

Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen durch?

Dies gilt z.B. bei einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten.

Falls „Ja“:

- haben Sie für die in diesen Fällen erforderliche Datenschutz-Folgenabschätzung in Ihrem Unternehmen einen Prozess eingeführt?

- Wer ist für diesen Prozess zuständig?

MELDE- UND BENACHRICHTIGUNGSPFLICHT

Haben Sie in Ihrem Unternehmen einen Prozess an die Aufsichtsbehörde eingeführt?

- Wer ist in Ihrem Unternehmen für die Meldung an die Aufsichtsbehörde zuständig?
- Sind die Beschäftigten hinreichend sensibilisiert?
- Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72-Stunden beachtet?
- Wer benachrichtigt die Betroffenen?
- Falls Sie eine(n) Datenschutz-beauftragte(n) bestellt haben, denken Sie an die Meldungvon seinen/ihren Kontaktdaten an die Aufsichtsbehörde

Gerne beraten wir Sie individuell.

Telefon +49 541 94422-0
info@pkf-wms.de

Stand: 5/2018

PKF WMS GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Steuerberater Rechtsanwälte

info@pkf-wms.de
www.pkf-wms.de