CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

CloudCommand

CyberSecurity im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Datenschutz-rechtliche Grundsätze

Die Grundsätze im Einzelnen

Bei den datenschutzrechtlichen Grundsätzen handelt es sich nicht lediglich um unverbindliche Programmsätze. Verstöße gegen datenschutzrechtliche Grundsätze können vielmehr nach Art. 83 Abs. 5 lit. a DSGVO mit dem nach der DSGVO maximalen Bußgeld geahndet werden.

Unternehmen sollten daher ihre Mitarbeiter mit den Grundsätzen der Datenverarbeitung vertraut machen.

Die Grundsätze im Einzelnen

Zu diesen Grundsätzen gehören insbesondere:

- Die Rechtmäßigkeit der Verarbeitung
- Verarbeitung nach Treu und Glauben (d.h. Fairness der Verarbeitung)
- Transparenz der Verarbeitung
- Zweckbindung (d.h. keine anlasslose Vorratsdatenspeicherung)
- Datenminimierung
- Richtigkeit der Daten
- Speicherbegrenzung

Die Grundsätze im Einzelnen

Diese Datenschutzgrundsätze stehen in keinem Rangverhältnis, sondern stehen gleichrangig nebeneinander. Trotzdem möchten wir hier insbesondere auf den Grundsatz der Transparenz hinweisen.

Dieser Grundsatz zieht sich wie ein roter Faden durch die gesamte DSGVO.

So sind die betroffenen Personen bei jeder Datenerhebung über Art und Umfang der Datenverarbeitung umfassend zu informieren.

Zudem steht ihnen ein Auskunftsrecht hinsichtlich des „ob“ und des Umfangs der Verarbeitung ihrer personenbezogenen Daten zu (Art. 15 DSGVO)

Die Grundsätze im Einzelnen

Eine transparente Verarbeitung kann zudem im Rahmen einer Interessenabwägung zwischen den berechtigten Interessen des Verantwortlichen und den schutzwürdigen Interessen der betroffenen Personen (Art. 6 Abs. 1 lit. f DSGVO) der ausschlaggebende Aspekt sein, aufgrund dessen eine Verarbeitung zulässig ist.

Unternehmen sollten daher das Transparenzgebot ernstnehmen, da sie dann regelmäßig deutlich weniger Probleme bei der Umsetzung der gesetzlichen Vorgaben der DSGVO haben als Unternehmen, die intransparent agieren.

Das sogenannte Accountability-Prinzip

Im Datenschutzrecht gilt gewissermaßen eine Beweislastumkehr zu Lasten des Verantwortlichen.

Dies beruht auf der „Rechenschaftspflicht“ aus Art. 5 Abs. 2, wonach der Verantwortliche in der Lage sein muss, die Einhaltung der Datenschutzgrundsätze nachweisen zu können.

Die Rechenschaftspflichten haben für Unternehmen nicht nur organisatorische, sondern auch ganz praktische Auswirkungen: Können bei einer Anfrage der Datenschutzaufsichtsbehörde erforderliche Informationen aufgrund mangelhafter Dokumentation nicht zur Verfügung gestellt werden, kann dies gem. Art. 83 DSGVO mit einem Bußgeld geahndet werden.

Das sogenannte Accountability-Prinzip

Konkretisiert wird die Rechenschaftspflicht durch folgende Regelungen:

- Pflicht zur Herstellung von Datensicherheit (Art. 24, 32 DSGVO)
- Erstellung interner Strategien zur Einhaltung der DSGVO (Erwägungsgrund 78 S. 2)
- Führen von Verarbeitungsverzeichnissen (Art. 30 DSGVO)
- Ggf. Erstellung einer Datenschutz-Folgenabschätzung bei riskanten Datenverarbeitungen (Art. 35 DSGVO)

Das sogenannte Accountability-Prinzip

Eine lückenhafte Dokumentation der Datenverarbeitung kann zudem im Fall einer Schadensersatzklage, die auf einen materiellen oder immateriellen Schaden durch einen DSGVO-Verstoß beruht, verheerende Folgen haben: Gem. Art. 82 Abs. 3 DSGVO müssen Verantwortliche und Auftragsverarbeiter den Nachweis fehlenden Verschuldens führen.

Durch eine nur lückenhafte oder im schlimmsten Fall nicht vorhandener Dokumentation wird ein solcher Nachweis nur schwerlich gelingen.

Das sogenannte Accountability-Prinzip

Die in der DSGVO normierten Datenschutzgrundsätze sind keine unverbindlichen Programmsätze, sondern für Unternehmen verpflichtend. Verstöße gegen Datenschutzgrundsätze werden mit dem höheren der beiden Bußgeldrahmen aus Art. 83 DSGVO belegt.

Im Datenschutzrecht gilt gewissermaßen eine Beweislastumkehr aufgrund der in Art. 5 Abs.2 DSGVO normierten Rechenschaftspflichten: Kommen Unternehmen diesen nicht nach, kann dies nicht zur zu einem Bußgeld durch die Datenschutzaufsichtsbehörde führen, sondern eine mangelnde Dokumentation verringert auch die Chance, sich erfolgreich gegen Schadensersatzansprüchen von Betroffenen zu wehren.

Dem datenschutzrechtlichen Transparenzgebot sollte besondere Beachtung geschenkt werden, da sich viele weitere Anforderungen aus der DSGVO direkt hieraus ableiten.

Welche weiteren Pflichten haben Unternehmen?

Das datenschutzrechtliche Pflichten für Unternehmen gehen über die Umsetzung der Anforderungen aus Art. 5 DSGVO hinaus. Die DSGVO enthält eine Vielzahl weiterer Pflichten, die von Verantwortlichen und teilweise auch von Auftragsverarbeitern umgesetzt werden müssen.

Welche weiteren Pflichten haben Unternehmen?

Die Wichtigsten sind:

- Erfüllung von Informationspflichten gegenüber Betroffenen (Art. 12 ff. DSGVO)
- Beantwortung von Betroffenenanfragen (Art. 15 bis 21 DSGVO)
- Melde- und Benachrichtigungspflichten bei Datenschutzvorfällen (Art. 33, 34 DSGVO)
- Abschluss von Auftragsverarbeitungsverträgen (Art. 28, 29 DSGVO)
- Erstellung eines Löschkonzepts (Art. 5, 17 DSGVO)
- Herstellung eines angemessenen Datenschutzniveaus bei Datentransfer in ein Drittland (Art. 46 ff. DSGVO)

Welche weiteren Pflichten haben Unternehmen?

Unternehmen werden ohne die Einführung eines Datenschutzmanagements kaum in der Lage sein die erforderlichen datenschutzrechtlichen Maßnahmen umzusetzen, um datenschutzkonform zu agieren und das Haftungsrisiko zu minimieren.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm