Die neue EU-Datenschutz-Grundverordnung

Bereits am 25.05.2016 ist die neue EU-Datenschutz-Grundverordnung „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ (DS-GVO) in Kraft getreten. Am 25.05.2018 endet die zweijährige Übergangszeit und die Verordnung wird bindende Vorschrift.
War der Datenschutz in der Vergangenheit nur selten ein Thema für Vorstände, Geschäftsführer und Führungskräfte, so hat sich dies geändert. Die DS-GVO nimmt diese Zielgruppe nicht nur in die Verantwortung, sondern geradezu ins Visier. Strafmaßnahmen und Haftungsrisiken in einer bis heute nicht vergleichbaren finanziellen Höhe sind die Folge. Der Bußgeld-Katalog orientiert sich dabei am europäischen Kartell- und Umweltrecht. Es können Bußgelder von bis zu 20 Mio. EUR oder ab einem Umsatz von 500 Mio. 4% des weltweiten Jahresumsatzes verhängt werden.

Betroffene Organisationen

Die DS-GVO gilt für jede Person oder Organisation, die personenbezogene Daten elektronisch in einer strukturierten Ablage verarbeitet. Ausgenommen sind nur Verarbeitungen im Rahmen persönlicher oder familiärer Tätigkeiten und einige staatliche Aktivitäten. Betroffen von der DS-GVO sind folglich:

- Unternehmen (unabhängig von der Rechtsform und Größe)
- Vereine,
- Verbände,
- Parteien,
- Stiftungen,
- Körperschaften des öffentlichen Rechts und
- Einrichtungen des Bundes, der Länder und Kommunen.

Die Vorschriften der DS-GVO sind von einem Ein-Personen-Unternehmen genauso einzuhalten wie von einem Konzern. Da Steuerklärungen elektronisch abgegeben werden müssen, können auch Vereine grundsätzlich eine elektronische Datenverarbeitung nicht vermeiden und sind demzufolge von der DS-GVO ebenfalls betroffen.

Wichtige operative-Neuerungen durch die DS-GVO

Betroffene, wie zum Beispiel Mitarbeiter, Kunden, Lieferanten und Partner, erhalten durch die Novellierung des Datenschutzrechtes Betroffenenrechte in nie zuvor gekanntem Ausmaß. So müssen beispielsweise alle Arbeitsverträge und Betriebsvereinbarungen auf Vereinbarkeit mit der DS-GVO geprüft und ggf. angepasst werden.
Neben den massiven Änderungen und Neuerungen gehören die Beweislastumkehrung zu Ungunsten der Unternehmen und Organisationen, die extrem umfangreichen Dokumentations- und Informationspflichten (ca. 20 neue Vorschriften) und die neue Auslegung der Verhältnismäßigkeit von Datenspeicherung zu den schwerwiegendsten Veränderungen. Zukünftig hat das verantwortliche Unternehmen die Pflicht, die Rechtmäßigkeit des Umgangs mit personenbezogenen Daten sowie das Vorhandensein einer wirksamen Datenschutzorganisation zu jedem Zeitpunkt nachweisen zu können (Accountability).

Beweislastumkehrung und Verbandsklagerecht

Gerade diese Beweislastumkehrung und die neuen anonymisierten Anzeigemöglichkeiten bedeuten für das verantwortliche Management neue Verantwortungen und erhebliche Haftungsrisiken.

Neben den neuen, umfangreichen Verbandsklagerechten für Verbände, Organisationen, Gewerkschaften und Verbraucherschutzorganisationen, besteht nicht zuletzt die Gefahr, dass diese Klagerechte auch missbräuchlich verwendet werden können, beispielsweise von Mitbewerbern, die sich so Wettbewerbsvorteile verschaffen wollen oder von zwielichtigen Rechtsanwälten, die auf Unterlassungsklagen ein Geschäftsmodell gründen.

Softwarenutzung

Im Hinblick auf die in den Unternehmen genutzten Softwarepakete, wie ERP-, CRM- oder gerade auch HRM-Systeme, ergeben sich umfangreiche und notwendige Veränderungsprozesse, um die neuen Betroffenenrechte und die Dokumentationspflichten umzusetzen. Oftmals sind vorhandene Datenspeicherungs- und Verarbeitungskonzepte zukünftig unzulässig und teilweise sogar strafbar.

Outsourcing (ADV)

Ist das Unternehmen an einem Outsourcingprozess beteiligt, etwa als Outsourcinggeber, als Outsourcingnehmer oder als Dienstleister/Subdienstleister in einem Outsourcingvorgang, so ergeben sich aus der zukünftig geltenden gesamtschuldnerischen Haftung vollkomme neue Haftungsrisiken. Es ist zukünftig nicht mehr möglich, in Vertragswerken das vollständige Haftungsrisiko für Datenschutzverstöße an Vertragspartner zu übertragen. Dieses gilt insbesondere auch für AGB und SLA-Konstrukte. Sämtliche Verträge mit externen Datenverarbeitern (ADV) müssen daher an die neue Gesetzgebung angepasst werden.

IT-Sicherheit

Für die IT besteht zukünftig die Pflicht zum Erstellen eines IT-Sicherheitskonzepts. Dieses muss eine wirksame Vorgehensweise definieren, die eine Verhinderung unbefugter Datenverarbeitung und die Einhaltung der Informations- und Dokumentationspflichten organisatorisch und technisch sicherstellt. Darüber hinaus muss ein Prozess zum Testen der Wirksamkeit der Schutzmaßnahmen entwickelt werden und die Nachweise hierüber regelmäßig dokumentiert werden. Ein weiterer Bestandteil des IT-Sicherheitskonzepts ist der verpflichtende Betrieb eines Meldeprozesses für Sicherheitsvorfälle. IT-Sicherheitsvorfälle müssen zukünftig zuverlässig erkannt, dokumentiert und entsprechend den unternehmensinternen Vorgaben behandelt werden.

Controlling

Der für die Unternehmensführung so wichtige Bereich des Controllings, mit sämtlichen Listen und erzeugten Reports muss auf Einhaltung der neuen Vorschriften durch die Gesetzgebung überprüft werden. Listen und Reports müssen überarbeitet und angepasst werden, damit sie den Betroffenenrechten Genüge leisten. Neue Reports müssen zukünftig grundsätzlich vor Erstellung auf Einhaltung der Gesetze geprüft werden. Eine spontane Listen- und Reportgenerierung gehört damit der Vergangenheit an.

Beschäftigtendaten im Personalbereich

Besondere Aufmerksamkeit verlangt der Umgang mit personenbezogenen Daten im Personalbereich. Auch hier greifen zwingend die Informations- und Dokumentationspflichten. Vorhandene Mitarbeiterinformationen sowie Mitarbeiterbestätigungen zum Datenschutz, Klauseln in Arbeitsverträgen oder Ergänzungen zum Arbeitsvertrag verlieren mit dem 25.05.2018 ihre Gültigkeit. Für jeden Mitarbeiter muss ein neues ergänzendes Vertrags- und Informationswerk aufgebaut werden. Durch besondere Zusätze in den Gesetzesgrundlagen wird es erforderlich sein, diese Informationen multikulturell und mehrsprachig aufzubereiten.

Unternehmensrisiko

Im Rahmen der hauseigenen Vorschriften und Vorgaben für das Risikomanagement muss das Unternehmensrisiko völlig neu bewertet werden. Die interne oder auch externe Revision erhalten neue Prüfszenarien und Regeln zur Vermeidung von Straftaten im Unternehmen, wie zum Beispiel SOX, müssen neu definiert werden. Dieses Risiko kann im schlimmsten Fall existenzbedrohend für das jeweilige Unternehmen sein.
Durch gezielte Information, Vorbereitung und Ausbildung aller Betroffenen minimieren Sie das Unternehmensrisiko.

Für weitere Fragen oder Beratung zur neuen DS-GVO stehe ich Ihnen gerne zur Verfügung:

Andreas Jensch, Geschäftsführer
Jastus GmbH
21614 Buxtehude

Tel.: 04161-736904
Mail: buero@jastus.de
Web: www.jastus.de

Jastus GmbH
Fachberatung für Informationssicherheit und Datenschutz