

WHITEPAPER

Digitalisierung, Datenschutz und IT – was tut sich 2024?

Die Zeit fliegt und wir befinden uns nun schon im April des Jahres 2024, das vor allem auf europäischer Ebene, aber auch auf nationaler Ebene, wieder zahlreiche rechtliche Änderungen im Bereich von Digitalisierung, Datenschutz und IT für Bürger und Unternehmer mit sich bringt. Wir haben im Folgenden die wichtigsten Neuerungen für Sie zusammengefasst:

Data Act

Seit 11.01.2024 ist die „Verordnung über die harmonisierten Vorschriften für einen fairen Datenzugang und eine faire Datennutzung“ (sog. „Data Act“, auf Deutsch „Datenverordnung“) in Kraft. Wirksam werden die Regelungen größtenteils aber erst ab 12.09.2025. Angesichts der tiefgreifenden Veränderungen ist diese lange Vorlaufzeit auch zwingend nötig.

Der Data Act regelt beispielsweise die Verpflichtung zur Weitergabe von Daten zwischen Unternehmern und Verbrauchern, von Unternehmen zu Unternehmen und – in einzelnen Fällen – auch an öffentliche Stellen. Diejenigen Unternehmen, die heute z.B. im Rahmen ihrer Produkte Daten von und für Kunden zu generieren, sind gezwungen, sich damit zu beschäftigen, ob und wie Kunden und Dritte hierauf Zugriff erhalten können.

Umgekehrt sollten sich Unternehmen, die bislang keine derartigen Daten nutzen, Gedanken machen, wie sie mögliche Datenzugriffsrechte auf „ihre“ Daten bei Herstellern und Dienstleistern erhalten und sinnvoll nutzen können.

Digital Services Act (DSA) und Digital Markets Act (DMA)

Der DSA, der seit dem 17.02.2024 anwendbar ist, schafft einen europaweit einheitlichen Rechtsrahmen für digitale Dienste wie Onlineplattformen und Suchmaschinen. Verpflichtete Online-Anbieter sind zum Beispiel Internetanbieter, Domännennamen-Registrierstellen, Hosting-Dienste wie Cloud- und Webhosting-Dienste, Online-Marktplätze, App-Stores, Plattformen der kollaborativen Wirtschaft und Social-Media-Plattformen, grundsätzlich unabhängig von ihrer Größe. Für sehr große Online-Plattformen und Suchmaschinen gelten besondere Vorschriften, weil diese besonderen Risiken für die Verbreitung illegaler Inhalte und für Schäden in der Gesellschaft bergen.

Der DSA nimmt die Anbieter insbesondere in die Pflicht, Vorkehrungen gegen rechtswidrige Inhalte zu treffen. Kommen die Online-Dienste diesen Verpflichtungen nicht nach, können Nutzer dies künftig bei der Bundesnetzagentur melden. Diese deutschen Besonderheiten werden mit dem „Digitale-Dienste-Gesetz“ (DDG) ergänzend zum DSA geregelt.

Der DSA ergänzt das bereits seit Mai 2023 gültige Gesetz über digitale Märkte (Digital Markets Act), das die Macht marktbeherrschender Digitalkonzerne beschränkt. Die EU-Kommission stellt darin einen Verhaltenskodex für große Digitalunternehmen auf. Für Zentrale Online-Plattformen wie zum Beispiel Suchmaschinen, soziale Netzwerke oder Online-Vermittlungsdienste gelten strengere Regeln: So werden sie zum Beispiel im Ranking nicht mehr eigene Angebote bevorzugen dürfen. Zuvor gab es nur in Deutschland mit dem GWB-Digitalisierungsgesetz, das 2021 in Kraft getreten ist, vergleichbare Regelungen.

NIS-2-Richtlinie („Network & Information Security / Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union)

Bislang in der Wahrnehmung angesichts der Bedeutung völlig unterschätzt: Die „NIS-2-Richtlinie („Network & Information Security / Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union)“.

Bis Oktober 2024 müssen betroffene Unternehmen einheitliche Cybersicherheits-Mindeststandards erfüllen (z.B. Einführung eines IT-Risikomanagements, Ableitung und Umsetzung technischer und organisatorischer Maßnahmen zur Erhöhung der IT-Sicherheit von Anlagen, Netzwerken, IT-Systemen und Lieferketten).

Direkt betroffen sind als sogenannte „Wesentliche Einrichtungen“ Unternehmen aus den Bereichen Energie, Straßen-, Schienen-, Luft- und Schiffsverkehr, Wasser, Digitale Infrastruktur und IT-Dienste, Bank- und Finanzwesen, Gesundheit, Öffentliche Verwaltung und Raumfahrt. Zudem als „Wichtige Einrichtungen“ Unternehmen aus den Bereichen Abfallwirtschaft, Post- und Kurierdienste, Chemische Erzeugnisse, Lebensmittel, Hersteller von Maschinen/Computern/Optik/Elektronik/Kraftfahrzeuge und Anhänger sowie Transportmittel, digitale Anbieter und Forschungseinrichtungen.

Auch ein Blick auf die einbezogenen Unternehmensgrößen zeigt, dass die Betroffenheit für viele Unternehmen schnell erreicht sein dürfte: Die Richtlinie gilt für Unternehmen ab 50 Mitarbeitern und mit mehr als 10 Millionen Euro Jahresumsatz. Und nachdem davon auszugehen ist, dass diese Unternehmen Pflichten aus der Richtlinie an Zulieferer und Dienstleister weitergeben werden, wird sie in den Lieferketten für weitaus mehr Unternehmen relevant werden. Hinzu kommt: Bis Oktober 2024 muss Deutschland ein NIS-2-Umsetzungsgesetz verabschiedet haben. Nach den bisherigen Diskussionen enthält dieses möglicherweise weitere Verschärfungen.

Cyber Resilience Act

Mit dem Cyber Resilience Act ist für das Jahr 2024 ein weiteres Regularium geplant, das alle Produkte mit digitalen Elementen (wie Smartwatches) betreffen soll. Hierdurch soll die Sicherheit von Produkten, die digital miteinander oder mit dem Internet verbunden sind, verbessert werden. Verpflichtet sollen alle Unternehmen sein, die Produkte mit digitalen Elementen herstellen, einführen oder damit handeln. Größenausnahmen für Unternehmen sind derzeit nicht geplant. Betroffene Unternehmen müssen die Produkte - bevor diese mit einem CE-Kennzeichen versehen werden dürfen - nach Kritikalität einordnen und hiernach risikoangemessene Cybersecurity-Maßnahmen (wie z.B. das Schließen von Sicherheitslücken während des gesamten Produktlebenszyklus) umsetzen. Auch sollen Nutzer zu Schwachstellen und Sicherheitsvorfällen verpflichtend informiert werden und europäische Behörden über ausgenutzte Schwachstellen unmittelbar in Kenntnis gesetzt werden müssen.

Überarbeitung der Produkthaftungsrichtlinie

Auch die aus dem Jahr 1985 stammende Produkthaftungsrichtlinie soll auf digitale Technologien hin angepasst werden. Der erweiterte Produktbegriff soll auch solche beweglichen Sachen, die in eine andere bewegliche oder unbewegliche Sache integriert sind, sowie Elektrizität, digitale Bauunterlagen und Software umfassen. Der Entwurf sieht Haftungsverschärfungen sowie Beweislast erleichterungen zu Gunsten von Geschädigten (ggfs. mit Offenlegungspflichten durch

die Unternehmen) vor. Die Richtlinie verstärkt somit die Produktbeobachtungs- und Dokumentationspflichten für Unternehmer, und zwar nicht nur aus dem Blickwinkel der Digitalisierung heraus.

Onlinezugangsgesetz (OZG)

Das Onlinezugangsgesetz, das den Rahmen für die weitere Digitalisierung der Verwaltung setzt sowie nutzerfreundliche und vollständig digitale Verfahren etablieren soll, wurde am 23.02.2024 novelliert. Durch die neuen Regelungen soll die Zusammenarbeit von Bund und Ländern intensiviert werden und eine einfache digitale Verfahrensabwicklung in einem übergreifenden Portalverbund ermöglicht werden.

Dafür will der Bund unter anderem zentrale Basisdienste, wie dem zentralen Nutzerkonto „BundID“ bereitstellen und so mittelfristig landeseigene Entwicklungen für Bürgerkontos und -postfächer ersetzen. Außerdem soll ein schriftformersetzendes qualifiziertes elektronisches Siegel für Unternehmen, vergleichbar mit der qualifizierten elektronischen Signatur für natürliche Personen, und eine Regelung zu „Digital-Only“ für Unternehmensleistungen eingeführt werden. Die Auswirkungen können sowohl für Bürger als auch Unternehmen als grundsätzlich positiv bewertet werden. So könnten z.B. Baugenehmigungen zukünftig deutschlandweit digital beantragt werden.

Ihr Ansprechpartner



Dr. Tobias Wagner

Partner
Rechtsanwalt

+49 911 40079914
wagner@thorwart.de