bureauPlattner

NEWSLETTER 10/2018

17.05.2018

IN DIESER AUSGABE

1 Die europäische Datenschutzverordnung UE/2016/679: neue Bestimmungen zur Verarbeitung personenbezogener Daten für Unternehmen

Für MwSt.-Subjekte

Mit 25. Mai tritt offiziell die europaweitgeltende Datenschutzverordnung („DSGVO") in Kraft. Die Verordnung ist in allen Mitgliedstaaten unmittelbar anwendbar und führt neben neuen Auflagen zur Datenverarbeitung auch neue Prinzipien ein, welche alle Unternehmen im Umgang mit personenbezogenen Daten befolgen müssen. Anders als bisher angenommen, werden die bereits existierenden nationalen Datenschutzbestimmungen (Gesetzesdekret vom 30. Juni 2003 Nr. 196, „Datenschutzkodex") – soweit sie mit den neuen Vorschriften vereinbar sind – weiterbestehen und Anwendung finden. Diese Anpassung des Datenschutzkodex an die EU-Verordnung soll mittels einer Durchführungsbestimmung geschehen, die nach eineinhalbmonatiger Geheimhaltung letzte Woche endlich an das Parlament und die italienische Aufsichtsbehörde für Datenschutz gesendet wurde. Die genannten Durchführungsbestimmungen müssen – wie vom europäischen Delegationsgesetz 2017 vorgesehen – innerhalb 21. Mai erlassen werden. Wobei zu bezweifeln ist, dass die italienische Regierung diese Frist einhalten wird.

Ab 25. Mai sollten italienische Unternehmen also im Stande sein, nachweisen zu können, sich an die Vorschriften gleich drei verschiedener Gesetzestexte angepasst zu haben.

Trotz der doch eher verwirrenden Gesetzeslage gibt es aber keinen Grund zur Panik, denn die italienische Datenschutz-Aufsichtsbehörde hat bereits versprochen, in den ersten Monaten nach Inkrafttretens der neuen Verordnung die neuen Auflagen in „ausgeglichener und pragmatischer" Weise anzuwenden.

Eine der wahrscheinlich größten Neuerungen der Verordnung ist die Einführung der Rechenschaftspflicht (sog. „Accountability-Prinzip"), wonach die Nachweispflicht der Einhaltung der Vorgaben der DSGVO ab sofort beim Unternehmen liegt.

Es gilt also, die neuen Auflagen und Verpflichtungen der Verordnung etwas besser kennenzulernen.

2 Liste der wichtigsten Verpflichtungen, die mit Wirksamwerden der Datenschutzverordnung eintreten [1]

Für MwSt.-Subjekte

Datenschutzerklärung (Artikel 13 und 14 DSGVO)	Der Verantwortliche der Datenverarbeitung – sprich das Unternehmen – hat eine Informationspflicht. Das bedeutet, dass im Falle einer Erhebung personenbezogener Daten, der betroffenen Person alle in Artikel 13 (und ggf. Artikel 14) angeführten Informationen mitgeteilt werden müssen. Maßnahmen: Datenschutzerklärung auffrischen oder ggf. neu aufsetzen.
Rechte der betroffenen Person (Artikel 15-18, 20, 21, 77)	Mit Inkrafttreten der DSGVO erhalten betroffenen Personen eine ganze Reihe neuer Rechte. Die betroffene Person muss über diese Rechte ausdrücklich Informiert werden und bei Bedarf in der Lage sein, diese Rechte jederzeit anzuwenden. Maßnahmen: notwendige technische und organisatorische Maßnahmen treffen, um die Geltendmachung der Rechte seitens der betroffenen Person zu gewährleisten.
Auftragsverarbeiter (Artikel 30)	Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern und auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments. Dieser Auftragsverarbeiter muss hinreichende Garantien dafür bieten, dass die Verarbeitungstätigkeiten im Einklang mit den Anforderungen des DSGVO erfolgen. Maßnahmen: Verträge mit Auftragsverarbeitern aufsetzen, in

	denen Gegenstand, Dauer, Art und Zweck der Verarbeitung sowie Pflichten und Rechte der Vertragsparteien festgelegt werden.
Verzeichnis der Verarbeitungstätigkeiten (Artikel 30)	Jeder Verantwortliche sowie deren Autragsverarbeiter müssen ein Verzeichnis aller Verarbeitungstätigkeiten führen, die ihrer Zuständigkeit unterliegen. Obwohl die Führung des Verzeichnisses nicht für Unternehmen und Einrichtungen gilt, die weniger als 250 Mitarbeiter beschäftigen, ist dessen Umsetzung auch in kleineren Betrieben im Zusammenhang mit den anderen Anforderungen und Grundsätzen der Verordnung ratsam. Maßnahmen: Verzeichnis erstellen, um Übersicht über den Datenfluss des Unternehmens zu bewahren (das Unternehmen muss in seiner Eigenschaft als Verantwortlicher und/oder Auftragsverarbeiter jeweils ein separates Verzeichnis führen).
Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde & Benachrichtigung an betroffenen Personen (Artikel 33 & 34)	Datenschutzverletzungen, welche zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge haben, müssen künftig der zuständigen Aufsichtsbehörde binnen 72 Stunden, nachdem die Verletzung bekannt wurde, mitgeteilt werden. Über Datenschutzverletzungen, welche unter Einschätzung des Verantwortlichen ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge haben, müssen auch die betroffenen Personen benachrichtigt werden. Maßnahmen: interne „Data Breach Policy" schaffen, die den genauen Ablauf einer Datenschutzverletzung regelt.
Datenschutzfolgenabschätzung (Artikel 35)	Hat eine bestimmte Form der Bearbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss der Verantwortliche vorab eine Abschätzung dieser Folgen durchführen. Maßnahmen: nur unbedingt notwendig für große Unternehmen und Verarbeitungstätigkeiten, die ein besonders hohes Risiko darstellen.

[1] Die Umsetzung und/oder Implementierung der angeführten Verpflichtungen ist je nach Dimension und Aktivität des Unternehmens nur bedingt notwendig.

3 Sanktionen für Verstöße gegen die Datenschutzverordnung

Für MwSt.-Subjekte

Wir erinnern daran, dass Verstöße gegen die Datenschutzverordnung, je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle der Maßnahmen der zuständigen Aufsichtsbehörde, die Verhängung einer Geldbuße von bis zu € 20.000.000 oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres mit sich tragen kann.
Wir weisen ausdrücklich darauf hin, dass es sich hierbei um den von der Verordnung vorgesehenen Höchstbetrag handelt und dass das exakte Strafausmaß dem Einzelfall entsprechend von der zuständigen Aufsichtsbehörde festgelegt wird.

Zusätzlich sieht der italienische Datenschutzkodex bereits eine Reihe von strafrechtlichen Sanktionen vor (z.B. eine Freiheitsstrafe zwischen 6 und 18 Monaten für die unrechtmäßige Verarbeitung von personenbezogenen Daten), welche die Durchführungsbestimmungen voraussichtlich weiter ausbauen werden.

Weiterführende Informationen können sie aus der im folgenden Link https://www.bureauplattner.com/wp-content/uploads/2018/05/GDPR.pdf beiliegenden Anlage entnehmen.

Bei weiteren Fragen bitte wenden Sie sich an unsere Berater RA Matteo Figini und Jakob Tasser, welche Sie gerne in der Umsetzung der erforderlichen Privacy-Maßnahmen unterstützen können.