Steuerberatung Röper
Betriebswirtschaftliche Beratung

Dipl. Kff. Jana Röper
Steuerberaterin
Fährstraße 16
18147 Rostock

Sonderausgabe zur EU-Datenschutz-Grundverordnung

Sehr geehrte Damen und Herren,

die sog. EU-Datenschutz-Grundverordnung ist am 25.05.2016 in Kraft getreten. Entsprechend einer darin geregelten Übergangsfrist kommt sie 2 Jahre nach ihrem Inkrafttreten zur Anwendung. Verpflichtend gilt die EU-Datenschutz-Grundverordnung also ***ab dem 25.05.2018****.*

Ab diesem Datum wird deren Einhaltung durch die EU-Datenschutzaufsichtsbehörden und die Gerichte überprüfbar sein. Sollten zu diesem Stichtag Ihre Prozesse nicht unternehmensspezifisch angepasst worden sein, und sollten in diesem Zusammenhang die Vorgaben der EU-Datenschutz-Grundverordnung nicht oder nicht in ausreichendem Maß umgesetzt worden sein, können ***empfindliche Sanktionen und Bußgelder*** *verhängt werden!*

Denn von den Regelungsinhalten sind nicht nur wir als Steuerberatungskanzlei betroffen, sondern auch Sie als unternehmerisch tätiger Mandant. Es entstehen ***neue Transparenzpflichten****, deren Einhaltung im Rahmen von Kontrollen der zuständigen Aufsichtsbehörde gegenüber nachgewiesen werden muss. Daher möchten wir Ihnen die wichtigsten Regelungsinhalte der EU-Datenschutz-Grundverordnung darstellen.*

Welche Prozesse und Daten sollten in Ihrem Unternehmen jetzt überprüft werden?

Die Datenverarbeitungsprozesse sollten im Unternehmen so dokumentiert werden, dass sie den Erweiterungen der Dokumentationspflicht bei der Auftragsverarbeitung gerecht werden: Möglichst mit zusätzlichen Funktionen zur Erkennung von Risiken.

Die Datenschutzerklärungen sollten an die erweiterten Informationspflichten angepasst werden. Insbesondere muss auch Ihre Unternehmens-Homepage angepasst werden.

Zudem müssen die entsprechenden Einwilligungserklärungen angepasst werden, damit diese den Verschärfungen der formalen Vorgaben gerecht werden, ebenso der Prozess für den Widerruf der Einwilligung. Die im Unternehmen vorhandenen Betriebsvereinbarungen müssen dahingehend überprüft werden, ob sie mit den Regelungsinhalten der Verordnung vereinbar sind in Form und Inhalt. Des Weiteren sollten die Prozesse zur Umsetzung von Widersprüchen angepasst werden, damit eine unverzügliche zeitliche Umsetzung gewährleistet ist. Ein besonderes Augenmerk sollte darüber hinaus auf die Prozesse gelegt werden, die sich mit der Meldung und Weitergabe aufgetretener

Datenverarbeitungspannen beschäftigen. Zudem sollten alle Daten in solchen Formaten gespeichert werden, in denen sie elektronisch an Dritte oder Aufsichtsbehörden übertragbar sind. Diese Formate sollten dann so hinterlegt sein, dass ein schnelles Auffinden gesuchter Dateien jederzeit problemlos möglich ist.

Welche Aufgaben sollte der Datenschutzbeauftragte in Ihrem Unternehmen erfüllen?

Die gesamte Steuerung sollte in der Abteilung Datenschutz bzw. beim Datenschutzbeauftragten angesiedelt sein. Ist diese Person aktuell in Ihrem Unternehmen noch nicht vorhanden, raten wir dringend, diese Position zeitnah zu besetzen. Der Datenschutzbeauftragte sollte dann damit betraut werden, zielgruppengerechte Schulungen hinsichtlich der am 25.05.2018 eintretenden Verordnung durchzuführen, die unternehmensbezogene Prozessoptimierung zu betreuen und die technisch und organisatorisch notwendig werdenden Maßnahmen zu überwachen. Und letztendlich sollte er dauerhaft die Entwicklungen der Verordnung auf nationaler und internationaler Ebene beobachten und die unternehmensinternen Prozesse dahingehend anpassen. Zu beachten ist weiterhin die sog. erweiterte Rechenschaftspflicht. Das bedeutet, die Verantwortlichkeit liegt unisono in Händen der jeweiligen Unternehmen. Alle Prozesse müssen so gestaltet werden, dass Prozesstransparenz eintritt, die jederzeit von den zuständigen Aufsichtsbehörden eingefordert werden kann. Sie müssen im Einzelfall jederzeit nachweisen können, dass gezielte Maßnahmen und Strategien von Unternehmensseite implementiert wurden. Kann dieser Nachweis nicht erbracht werden, hat dies schwerwiegende Auswirkungen auf die Höhe des Bußgelds.

Die Datenschutzaufsichtsbehörden erhalten zur Durchsetzung umfangreiche Befugnisse und haben demgemäß ihre Personalkapazitäten aufgestockt. Flankiert werden die erweiterten Befugnisse durch eine Ausweitung des Bußgeldrahmens bei Verstößen. Bisher konnten max. 300.000 € als Bußgeld festgesetzt werden. Zukünftig sind Bußgelder bis 20 Millionen € oder 4 % vom Jahresumsatz zulässig, wobei der jeweils höhere Wert gilt.

Die DSGVO findet Anwendung auf die Verarbeitung personenbezogener Daten natürlicher Personen, ohne dies genauer zu definieren. Im Zweifel sollte, z. B. bei der Speicherung einer IP-Adresse, vom Personenbezug ausgegangen werden.

Anzuwenden sind die Datenschutzbestimmungen, wenn die Verarbeitung der Daten im Rahmen der Tätigkeiten einer Niederlassung in der EU erfolgt. Die Verarbeitung selbst kann auch außerhalb der EU stattfinden. Hat ein Unternehmen seine Niederlassung außerhalb der EU, muss es die Regelungen trotzdem beachten, wenn es Waren oder Dienstleistungen in der EU anbietet und die Datenverarbeitung mit seinem Angebot zusammenhängt.

*Folgende **Grundprinzipien** sind zu beachten:*

- ***Verbot mit Erlaubnisvorbehalt**: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, es liegt eine Einwilligung oder eine in der DSGVO normierte Ausnahme vor. Eine solche Ausnahme kann z. B. die Verarbeitung zur Erfüllung eines Vertrags oder zur Erfüllung einer rechtlichen Verpflichtung sein.*

- ***Datensparsamkeit**: Die Verarbeitung personenbezogener Daten muss auf das für den Zweck der Verarbeitung notwendige Maß beschränkt sowie dem Zweck angemessen und sachlich relevant sein.*

- ***Zweckbindung**: Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden.*

- ***Datensicherheit**: Der Unternehmer hat geeignete technische und organisatorische Maßnahmen zur Datensicherheit umzusetzen. Dabei hat er neben dem Stand der Technik und den Implementierungskosten, den Zweck der*

Datenverarbeitung, aber auch die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die persönlichen Rechte zu berücksichtigen. Eine Verletzung des Schutzes personenbezogener Daten muss der Unternehmer unverzüglich, nach Möglichkeit innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls, an die zuständige Datenschutzbehörde melden. Es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen.

· ***Betroffenenrechte**: Unternehmen haben gegenüber den Betroffenen weitreichende Informationspflichten zu erfüllen, z. B. über den Zweck und die Rechtsgrundlage der Datenverarbeitung. Sie müssen gegenüber einer anfragenden Person Auskunft darüber geben, ob und ggf. welche Daten dieser Personen sie verarbeitet haben. Darüber hinaus können Betroffene von Unternehmen verlangen, dass unzutreffende personenbezogene Daten berichtigt oder Daten gelöscht werden, weil z. B. die Einwilligung zur Datenverarbeitung widerrufen wurde.*

· ***Datenschutz-Folgenabschätzung**: Diese muss der Unternehmer vorab vorsorglich durchführen, wenn die Art der Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten birgt.*

· ***Datenschutzbeauftragter**: Ein Datenschutzbeauftragter ist u. a. zu benennen, wenn ein deutsches Unternehmen mehr als zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt. Muss ein Unternehmen eine Datenschutz-Folgenabschätzung durchführen, ist ein Datenschutzbeauftragter unabhängig von der Anzahl der Beschäftigten, die personenbezogene Daten verarbeiten, zu benennen.*

Das neue Datenschutzrecht beinhaltet umfangreiche und detaillierte Pflichten für Unternehmen. Es müssen interne Prozesse angepasst bzw. neu etabliert werden. Auch eine Schulung der Mitarbeiter ist unerlässlich. Unternehmen sollten unverzüglich, ggf. unter Hinzuziehung ihres Rechtsberaters oder eines Datenschutz-Dienstleisters, mit der Umsetzung beginnen.

In einem individuellen persönlichen Gespräch erläutern wir Ihnen gerne alle Teilaspekte, die für die Umstellung Ihrer unternehmensinternen Prozesse erforderlich sind, um den Inhalten der Verordnung gerecht zu werden. Wir freuen uns auf das Beratungsgespräch!

Mit freundlichen Grüßen

Jana Röper
Steuerberaterin

Anhang: Die wichtigsten Regelungsinhalte der EU-Datenschutz-Grundverordnung

Suchdienste und soziale Netzwerke einbezogen

Der Geltungsbereich der Verordnung wird auf alle Datenverarbeitungen ausgeweitet, die sich an EU-Bürger richten und die personenbezogene Daten von EU-Bürgern verarbeiten. Bemerkenswert ist darüber hinaus, dass auch bei Suchdiensten und sozialen Netzwerken die Verordnung Anwendung findet. Sogar der Tourist, der nach Deutschland kurzfristig urlaubsbedingt einreist, fällt für diesen Zeitraum unter die Regelungsinhalte der Verordnung, sofern in Deutschland ansässige Unternehmen seine Daten speichern und verarbeiten. Auch finden sich in der Verordnung eine ganze Reihe neuer Begriffe wie z. B. "umfassende Verarbeitung" oder "Profiling". Auch neue Definitionen sind zu finden, für die Begriffe "biometrische Daten" und "genetische Daten". Diesen Definitionen sollte insbesondere von denjenigen Unternehmen besondere Beachtung geschenkt werden, die z. B. mit Gesichtserkennung oder Erkennungsverfahren über den Fingerabdruck arbeiten.

Altersgrenze von Kindern beachten

Kinder genießen im Rahmen der EU-Datenschutz-Grundverordnung einen besonderen Schutz. Sofern Ihr Unternehmen in verschiedenen EU-Mitgliedstaaten tätig ist, sollten Sie individuell prüfen, welche Altersgrenzen dort jeweils gelten. Denn die Beweispflicht für die Einwilligung von Kindern oder deren Erziehungsberechtigten bezüglich Datenschutz liegt beim Unternehmen.

Widerruf der erteilten Einwilligung deutlich einfacher

Der Widerruf der erteilten Einwilligung wurde in seinen Anforderungskriterien deutlich herabgesetzt. Hat der Betroffene zunächst seine Einwilligung zur Speicherung und Verarbeitung seiner personenbezogenen Daten zugestimmt, so kann er diese Einwilligung jederzeit und ohne Begründung widerrufen. Hierbei muss unternehmensspezifisch darauf geachtet werden, dass der Widerruf für den Betroffenen mindestens so einfach gestaltbar ist wie die erteilte Einwilligung. Das bedeutet, dass Webseiten, Apps und andere vom Unternehmen angebotene digitale Dienste so gestaltet sind, dass sie den Vorgaben der EU-Datenschutz-Grundverordnung entsprechen.

Kopplungsverbot verschärft

Auch das sog. Kopplungsverbot wurde verschärft. Nach bisher geltendem Recht durfte der Abschluss eines Vertrags uneingeschränkt mit einer erteilten Einwilligung hinsichtlich der Speicherung und Verarbeitung der personenbezogenen Daten des Vertragspartners gekoppelt werden. Mit Inkrafttreten der Verordnung kann es notwendig werden, denselben Vertrag einmal mit und einmal ohne die zu erteilende Einwilligung zur Speicherung und Verarbeitung der personenbezogenen Daten anzubieten.

Informations- und Auskunftspflichten ergänzt

Die sog. Informations- und Auskunftspflichten wurden um weitere Angaben ergänzt. Ihr Unternehmen muss dem Betroffenen zukünftig eine Reihe weiterer Informationen zur Verfügung stellen. Dazu gehören insbesondere Informationen zu der Rechtsgrundlage, auf die sich die unternehmensspezifische Datenverarbeitung stützt. Auch Angaben zur Dauer der Speicherung müssen gemacht werden. Zusätzlich muss beachtet werden, dass es jede Form der Weiterverarbeitung der Daten zu einem anderen Zweck zukünftig erforderlich macht, dass dem Betroffenen erneute Informationen zur Verfügung gestellt werden.

Portabilitätsverpflichtungen einhalten

Auch gibt es für die erhobenen und gespeicherten Datensätze sog. Portabilitätsverpflichtungen. Das Unternehmen, das die Daten gespeichert und verarbeitet hat, die der Betroffene ihm zur Verfügung gestellt hat, muss diese gegebenenfalls in einem gängigen Format wieder zur Verfügung stellen und auf Wunsch so aufbe-

reiten, dass sie jederzeit an Dritte weitergegeben werden können. Das stellt insbesondere für alle Unternehmen eine große Herausforderung dar, die mit elektronischen Plattformen arbeiten.

Löschpflicht, Hinweispflicht und Widerspruchsrecht erweitert

Des Weiteren werden die sog. Löschpflicht und die Hinweispflicht bei Weitergabe von Daten an Dritte erweitert. Das birgt insbesondere dann Brisanz, wenn ein Unternehmen veraltete Datenbestände an Dritte weitergereicht hatte. Es ergibt sich die unternehmerische Pflicht, diese Daten zu korrigieren und diesen Korrekturbedarf an das entsprechende Unternehmen weiterzuleiten. Für Ihr Unternehmen bedeutet das, dass möglichst bereits schon jetzt darauf geachtet werden sollte, welche personenbezogenen Daten Ihr Unternehmen verarbeitet, woher diese Daten stammen und an wen Sie diese Daten weitergeben. Andernfalls wird es sehr schwierig sein, den Vorgaben der EU-Datenschutz-Grundverordnung gerecht zu werden! Auch sollten Sie das unternehmensspezifische Löschverfahren dahingehend überprüfen, ob es tatsächlich jederzeit möglich wäre, bei einem geltend gemachten Löschanspruch die Daten zügig aufzufinden und zu löschen.
Ebenso wird das Widerspruchsrecht deutlich erweitert. Der Betroffene kann insbesondere der Datenverarbeitung seiner Daten widersprechen, wenn diese zu Zwecken des Direktmarketings, einschließlich der Profilbildung für diese Zwecke genutzt werden sollen. Hier gilt es vonseiten des Unternehmens darauf zu achten, dass der Betroffene explizit und separiert von jeglicher Art anderer Information darauf hingewiesen wird, dass dieses Recht besteht.

Meldepflichten bei Datenpannen verschärft

Auch werden die sog. Meldepflichten bei Datenpannen deutlich verschärft. So ist jedes Unternehmen zukünftig dazu verpflichtet, jeden Vorfall, der ein Risiko für die Rechte und Pflichten der Betroffenen darstellt, innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde zu melden. Zudem muss auch der Betroffene selbst unverzüglich über die aufgetretene Datenpanne informiert werden, wenn diese voraussichtlich zu einem hohen Risiko für ihn führt. Gerade in diesem sehr sensiblen Bereich sollte Ihr Unternehmen Richtlinien und Verfahren entwickeln, die eine unverzügliche Meldung solche Datenpannen zeitnah gewährleisten. Wir unterstützten Sie bei der Entwicklung solcher Richtlinien gerne.
Dabei sollte zwingend auf die erforderlichen Mindestinhalte geachtet werden, die sich aus der DS-GVO ergeben. Darüber hinaus ist jedes Unternehmen verpflichtet, die Datenpannen unternehmensintern zu dokumentieren.

Zuständige Aufsichtsbehörde

Zu beachten ist weiterhin, dass sich die zuständige Aufsichtsbehörde für ein europaweit tätiges Unternehmen nach dem Hauptsitz oder nach der Niederlassung richtet, die generell über Datenverarbeitung entscheidet. Bei international tätigen Unternehmen sollte demnach zwingend eine Zuordnung getroffen werden, an welcher Örtlichkeit die maßgeblichen Entscheidungen hinsichtlich der Verarbeitung personenbezogener Daten getroffen werden.

Freiwilligkeit der Erklärung

Es werden auch erhöhte Anforderungen an die sog. Freiwilligkeit der Erklärung gestellt. Die Einwilligung zur Speicherung der Daten erfordert bei demjenigen, von dem sie eingefordert werden, eine freiwillige, spezifisch informierte und eindeutige Handlung. Dies kann online z. B. durch das bewusste Anklicken eines Kästchens erfolgen.

Keine ordnungsgemäß erteilte Einwilligung läge insbesondere dann vor, wenn ein sog. stillschweigendes Einverständnis vorausgesetzt würde, z. B. durch ein bereits standardmäßig vorab angekreuztes Kästchen. Sind in den Prozess sogar verschiedene Datenverarbeitungsvorgänge eingebunden, muss in jeden einzelnen dieser Prozesse gesondert eingewilligt werden. Es muss im Einzelnen sogar vom Unternehmen der Nachweis er-

bracht werden, dass eine effektive Einwilligung gegeben wurde! Diese Einwilligung kann elektronisch abgegeben werden.

Datenschutz-Folgenabschätzung

Für besonders risikobehaftete Datenverarbeitungen kann die Durchführung einer sog. Datenschutz-Folgenabschätzung vorgeschrieben werden. Muss selbige im Unternehmen durchgeführt werden, sollte dieser ein entsprechendes Risikomanagement zugrunde liegen. Eine risikobehaftete Datenverarbeitung liegt insbesondere dann vor, wenn man zu dem Ergebnis gelangt, dass ein hohes Risiko für die Rechte und Freiheiten des Betroffenen besteht. Auch die Einführung neuer Technologien begründet die Implementierung einer Datenschutzfolgeabschätzung.