der Betroffenen (deren Daten verarbeitet werden) gewährleistet wird. Dies sollte bei Servern innerhalb der EU grundsätzlich kein Problem darstellen. Auftragsverarbeiter können ihre Zuverlässigkeit/Geeignetheit zukünftig durch die Einhaltung genehmigter Verhaltensregeln oder durch eine entsprechende Zertifizierung nachweisen. Da diese Zertifizierungspraktiken neu sind, ist jedoch erst mittelfristig mit derartigen Nachweisen zur rechnen. Bis dahin müssen die Unternehmen den Dienstleister und seine Geeignetheit ´selbst bewerten.

Was müssen Unternehmen/Betriebe für ihre Webseiten beachten?
Die Unternehmen sollten, wie bereits bisher erforderlich, eine Datenschutzerklärung auf den jeweiligen Webseiten aufführen. Neu ist, dass zudem entsprechend den Informationspflichten nach Art. 13 DS-GVO ebenfalls informiert werden muss. Dies ist in den meisten Fällen erforderlich, da üblicherweise die modernen Webseiten mit Webanalysediensten, Kontaktformularen, etc. ausgestattet sind.


Foto: agiles

„Bestimmte Prozesse innerhalb der Lieferkette müssen überarbeitet werden“

Software ► Mit der Einführung der neuen Datenschutz-Grundverordnung (DS-GVO) stellen sich für Unternehmen Herausforderungen in Bezug auf die technische Umsetzung der Änderungen. Das Fruchthandel Magazin sprach mit Christian Sega, Geschäftsführer der agiles Informationssystems GmbH, über Neuerungen und Vorgaben.

Christian Sega, Geschäftsführer der agiles Informationssystems GmbH

Wie sind Unternehmen aus den Bereichen Food und Handel von den Änderungen der EU-Datenschutz-Grundverordnung betroffen?
Christian Sega: Aufgrund der der neuen Datenschutz-Grundverordnung (DS-GVO), die am 25. Mai 2018 in Kraft tritt, ist das Thema Datenschutz in Deutschland zurzeit allgegenwärtig. Aber auch zuvor zählte Deutschland zu den Ländern mit den strengsten Auflagen, wenn es um den Schutz personenbezogener Daten geht. Dennoch ersetzt die neue DS-GVO das bestehende Bundesdatenschutzgesetz vollumfänglich – und dies in ganz Europa.

Die wichtigsten Änderungen durch die DS-GVO:
- Personen und Unternehmen erhalten mehr Rechte (z.B. das Recht auf Informationspflicht beim Auskunftsersuchen)
- Verstöße gegen den Datenschutz werden zukünftig erheblich schärfer bestraft
- Die Höchststrafe liegt bei bis zu vier Prozent des (Konzern-) Jahresumsatzes oder bis zu 20 Mio Euro
- Unternehmen unterliegen einer Dokumentations- und Auskunftspflicht

Die neuen Richtlinien sind bindend für alle, auch für Unternehmen aus den Bereichen Food und Handel, die Daten von EU-Bürgern nutzen und diese verarbeiten oder speichern. Grundsätzlich gibt es keine Unterscheidung zwischen den Branchen – es sind alle Unternehmen betroffen, die personenbezogene Daten verarbeiten. Jedoch existieren Abstufungen für z.B. Unternehmen, die weniger als 250 MA beschäftigen.
Allerdings ist vielen Handelsunternehmen nicht bewusst, dass bestimmte Prozesse und Datenübertragungen innerhalb der Lieferkette überarbeitet werden müssen. Zum Beispiel bilden einige Logistik- und Handelsunternehmen nicht die gesamte Lieferkette ab. Häufig gibt

es verschiedene Sub-Unternehmen, die Aufgaben in Bereichen wie Transport oder Lagerung übernehmen. Die verschiedenen Unternehmen arbeiten heutzutage oft mit Schnittstellen zwischen den jeweiligen Softwarelösungen und (externen) Organisationseinheiten, so dass jederzeit alle beteiligten Unternehmen einen Überblick über die Lieferkette und den aktuellen Status der Ware haben. Diese Daten enthalten in vielen Fällen jedoch auch personenbezogene Informationen, unter anderem die Adresse des Kunden, Ansprechpartner beim Sub-Unternehmer oder auch den Namen des Lieferanten/Fahrers etc. Oft werden die Daten auch in Form von Emails ausgetauscht – auch hier gelten künftig spezielle Aufbewahrungs- und / oder Löschvorschriften.

Foto: ©IckeT - stock.adobe.com

Welche Maßnahmen empfehlen Sie Unternehmen, um den Vorgaben dieser Verordnung zu entsprechen?

Welche Prozesse angepasst werden müssen, hängt von den individuellen Vorgängen der Unternehmen ab. In jedem Fall ist eine ausführliche Recherche der Richtlinien anhand verlässlicher Quellen unabdingbar. Die Annahme, dass kleinere Unternehmen weniger stark betroffen sind als Konzerne, ist in den meisten Fällen falsch. Gleichzeitig sollte sich jedes Unternehmen darüber im Klaren sein, dass es sich nicht um eine einmalige Umsetzung zum 25. Mai handelt. Der Umgang mit personenbezogenen Daten sollte regelmäßig überprüft werden – es handelt sich also um einen kontinuierlichen Arbeitsprozess.

Ein konkretes Beispiel ist § 15 Abs. 1 DS-GVO, nach dem Betroffene das Recht haben, zu erfragen, ob und welche personenbezogenen Daten verarbeitet werden. Bei der Umsetzung dieser Richtlinie kann z.B. eine Software helfen, mit der ein vollständiges Reporting einschließlich aller Stamm- und Bewegungsdaten erstellt werden kann. Dies schließt auch Drittlösungen ein, die mit dem System verbunden sind, beispielsweise Add-Ons oder angebundene Cloud-Services. Auch Mail-Programme, CRM-Systeme oder andere Systeme sind davon betroffen.

Außerdem wird in der Datenschutzgrundverordnung die „Verschlüsselung" (in Form von unkenntlich machen) personenbezogener Daten sowie der Schutz vor unbefugtem Zugang verlangt. Damit soll ein dem Risiko angemessenes Schutzniveau gewährleistet werden. Unternehmen benötigen daher ein umfangreiches Sicherheitskonzept, welches ausführlich dokumentiert sein sollte – dazu gehören auch unterschiedliche Zugriffsrechte einzelner Mitarbeiter. Darüber hinaus ist in Betrieben ab zehn Mitarbeitern grundsätzlich ein Datenschutzbeauftragter vorgeschrieben. Dieser kann auch über einen externen, zertifizierten Datenschutzbeauftragten gestellt werden.

> „Vielen Unternehmen ist nicht bewusst, dass bestimmte Prozesse überarbeitet werden müssen."
>
> Christian Sega

Prüfen sollten Unternehmen zudem eine Überarbeitung der sog. Auftragsdatenverarbeitungs-Verträge (AV). Dies betrifft Firmen, die personenbezogene Daten im Auftrag, also von einem Dienstleister verarbeiten lassen. Zu diesen Dienstleistern zählen z.B. auch IT-Beratungsfirmen und Software-Hersteller im Rahmen von Support- oder anderen Dienstleistungen.

Die neuen Richtlinien der DS-GVO sind auch bindend für Unternehmen aus den Bereichen Food und Handel, die Daten von EU-Bürgern nutzen und diese verarbeiten oder speichern.

Gibt es besondere rechtliche Vorgaben für die Nutzung von Cloud-Diensten? Wie können diese eingehalten werden?

Cloud-Lösungen sind heute ein fester Bestandteil der IT-Infrastruktur. Auch für die personenbezogenen Daten, die in einer Cloud gespeichert sind, gelten ab dem 25. Mai strenge Vorgaben für eine Auftragsverarbeitung. Jedoch sollte auch bedacht werden, dass die DS-GVO viele Aspekte beinhaltet, die auch vorher bereits im Datenschutzrecht enthalten waren.

Umgang mit Clouds

Der Umgang mit Daten in der Cloud in Bezug auf die neuen Regelungen ist ein besonderer Fall. Auch wenn die gesamte IT-Struktur aus einer Cloud bezogen wird oder virtuelle Maschinen zum Einsatz kommen, kann die Verantwortung für die Daten nicht vollständig an einen Drittanbieter abgetreten werden. Der Auftraggeber der Datenverarbeitung, also das Unternehmen, der Freiberufler oder die Organisation, die Daten in der Cloud speichern lassen, dürfen sich nicht einfach auf ihre Cloud-Dienstleister und dessen Datenschutzanspruch verlassen. Dabei entsteht ein grundsätzliches Problem: Für viele Auftraggeber ist es schwierig, sich ein genaues Bild von den tatsächlich bei ihrem Dienstleister vorhandenen technischen und organisatorischen Schutzmaßnahmen (sog. TOM's) zu machen.

Ein Datenleck kann jederzeit passieren. Eine Schutzmaßnahme ist die Verschlüsselung.

Deswegen sieht die DS-GVO eine verstärkte Nutzung von Zertifikaten vor, die dann beispielsweise andere Nachweise zu den technischen und organisatorischen Sicherheitsvorkehrungen der Cloud-Dienstleister ersetzen (sog. Konformitätserklärungen).

Ein klares Hauptaugenmerk der neuen DS-GVO ist die Dokumentations- und Informationspflicht. Unternehmen, die die Dienste von Cloud-Anbietern nutzen, müssen zunächst mit dem Dienstleister gemeinsame Compliance-Regeln abstimmen. Aus Sicht eines Unternehmens ist es sinnvoll, die Regeln und Änderungen vertraglich festzuschreiben. Selbstverständlich gibt es eine ganze Reihe weiterer Maßnahmen, um einen DS-GVO-konformen Umgang mit personenbezogenen Daten zu gewährleisten. Beschäftigen sollten sich Unternehmen unter anderem mit folgenden Themen:

- Dokumentationspflicht: Diese umfasst Informationen zum Zweck der Datenverarbeitung, Aufbewahrungsfristen sowie die unternehmensinternen Empfänger der Daten.
- Unternehmen müssen ihre Kunden umfangreich über die Umstände aufklären, unter denen sie Daten erheben, speichern und verarbeiten.
- Es müssen Verfahren eingeführt werden, die das ausdrückliche Einverständnis der Betroffenen garantieren (sog. Verfahrensverzeichnisse).
- Schutz: Ein Datenleck kann jederzeit passieren. Eine Maßnahme, die ausreichend Schutz bietet, ist die Verschlüsselung. Anwender sollten Daten daher noch vor der Migration in z.B. Cloud-Lösungen verschlüsseln oder separate Verschlüsselungssoftware einsetzen (z.B. für Emails etc.). Darüber hinaus gibt es eine Meldepflicht der Cloud-Anbieter bei Datenpannen und -diebstahl.
- Haftung: Bislang waren Auftraggeber allein verantwortlich für die von ihnen initiierte Datennutzung. Jetzt sieht die DS-GVO eine gemeinsame Haftung des sog. „Hostes" und des Auftragsgebers gegenüber den Betroffenen vor, sowohl für materielle als auch immaterielle Schäden. Nach der DS-GVO können Betroffene dabei sogar direkt rechtlich gegen den Cloud-Dienstleister vorgehen, wenn sie der Meinung sind, dass ihre Rechte infolge einer unzureichend abgesicherten Datenverarbeitung bei den Cloud-Dienstleistern verletzt wurden.
- Neues Recht auf Datenübertragbarkeit: Auftraggeber haben einen Anspruch darauf, dass sie betreffende personenbezogene Daten in einem strukturierten, gängigen und maschinenlesbaren Format abrufen können und diese Daten zu anderen Anbietern übertragen können.

Unternehmen müssen ihre Kunden künftig umfangreich über die Umstände aufklären, unter denen sie Daten erheben, speichern und verarbeiten.

Hinweis: Die Datenschutz-Grundverordnung ist ein komplexes Thema. In vielen Bereichen sehen Rechtsexperten Interpretationsbedarf hinsichtlich der konkreten Auslegung im Unternehmensalltag. Die in diesem Beitrag dargestellten Informationen sind allgemeiner Art und stellen keine Rechtsberatung dar. Unternehmen sollten zur Lösung von konkreten Rechtsfällen einen IT-Fachanwalt oder Ihren Datenschutzbeauftragten konsultieren. ●

TÜV SÜD

Verbesserte Auskunftsrechte für Betroffene

Beim Thema „Auskunftsrechte" im Rahmen der neuen DS-GVO hat sich für Kunden oder Online-Nutzer einiges getan. TÜV SÜD weist darauf hin, dass für diese nun ein erweitertes Auskunftsrecht für ihre Daten gilt, das heißt, Firmen müssen über alle gespeicherten personenbezogenen Daten Auskünfte erteilen. Wenn gewünscht, sind Unternehmen sogar verpflichtet, Daten ganz zu löschen.

Das Auskunftsrecht untergliedert sich in zwei Stufen. Zunächst können betroffene Personen Informationen darüber verlangen, ob überhaupt personenbezogene Daten von ihnen verarbeitet werden. Wenn dies der Fall ist, besteht grundsätzlich ein Recht auf Auskunft über diese Daten. Firmen müssen außerdem mitteilen, wie lange sie die personenbezogenen Daten speichern werden und welche Kriterien zur Festlegung dieser Zeitspanne geführt haben. Hinzu kommt, dass Betroffene die Berichtigung oder Löschung ihrer Daten verlangen dürfen. Auch können sie verfügen, dass diese Daten nur eingeschränkt verarbeitet werden dürfen. Über dieses Widerspruchsrecht sowie ihr Beschwerderecht bei einer Aufsichtsbehörde müssen Betroffene ebenfalls informiert werden. Artikel 15 DSGVO erweitert somit die bisher bekannten Regelungen des § 34 BDSG bei den Auskunftsrechten.

Durch das erweiterte Beschwerderecht für Betroffene ist damit zu rechnen, dass diese häufiger von ihrem Recht Gebrauch machen und beispielsweise auf Löschung ihrer Daten bestehen. TÜV SÜD weist darauf hin, dass Verantwortliche – sofern noch nicht geschehen – konkrete Datenlöschprozesse implementieren müssen.