HLB Deutschland GmbH
Wirtschaftsprüfungsgesellschaft

LKC.

## ERP im Kontext der Datenschutz-Grundverordnung:

# Fluch oder Segen?

**Ein Beitrag von Peter Jordan**

Es steht eine Neuerung auf dem Datenschutz-Sektor bevor, die Unternehmen in der ganzen Europäischen Union betrifft. Die Rede ist von der Datenschutz-Grundverordnung (DS-GVO). Diese Neuregelung soll die Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen vereinheitlichen. Anlässlich dieser Änderung stellen sich Unternehmen und öffentliche Behörden die Frage, was für sie bei der DS-GVO zu beachten ist.

### Die Entstehung der DS-GVO

Nach zähen Verhandlungen wurde die DS-GVO am 14. April 2016 vom EU-Parlament beschlossen. Die Verordnung ist zum 25. Mai 2016 in Kraft getreten und wird ab dem 25. Mai 2018 in allen Mitgliedstaaten der EU unmittelbar gelten und damit Teil der nationalen Rechtsordnung sein. Doch im Zuge des Harmonisierungsprozesses sind viele aktuelle Herausforderungen des Datenschutzes auf der Strecke geblieben. So stellen sich sowohl die zur Anwendung aufgeforderten Unternehmen, als auch Rechtsexperten viele Fragen, die es noch zu beantworten gilt.

### Die drei grundsätzlichen Ziele der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung verfolgt zunächst das primäre Ziel, das unübersichtliche Datenschutzrecht der einzelnen Mitgliedsstaaten zu vereinheitlichen. Da sie in allen europäischen Staaten direkte Anwendung finden wird, soll ein einheitliches Datenschutzregime im gesamten europäischen Raum entstehen. Eine weitere Umsetzung der DS-GVO durch nationale Gesetzgeber ist nicht nötig. Der generelle Harmonisierungsgedanke der EU spielt hierbei also eine tragende Rolle.

Zweitens soll durch die DS-GVO für gleiche wirtschaftliche Rahmenbedingungen in der Europäischen Union gesorgt werden. Das Ziel war, die seit 1995 geltende EU-Datenschutzrichtlinie durch eine einheitliche Verordnung abzulösen, die nunmehr nach 20 Jahren das Datenschutzrecht auf eine neue, einheitliche Basis stellt. Diese Vereinheitlichung soll auf langfristige Sicht auch zu einer Stärkung des Binnenmarktes führen.

Als drittes Ziel soll der Datenschutz in Europa auf Grund der anwachsenden Herausforderungen durch Cloud Computing, Big Data, Soziale Medien und Suchmaschinen modernisiert werden. Dabei soll der Grundrechtsschutz des Einzelnen im Vordergrund der Modernisierung stehen. Diese Umgestaltung ist angesichts der vielfältigen neuen technischen Anwendungen dringend erforderlich, da sie den Schutz natürlicher Personen und den freien Verkehr gewährleisten soll.

Diese Thesen beziehen sich auf die angestrebten, gesetzgeberischen Ziele, welche die DS-GVO verfolgt. Doch was müssen die Unternehmen und die öffentlichen Stellen selbst bei der neuen Grundverordnung beachten?

**Der Anwendungsbereich der DS-GVO**

Unternehmen müssen einen Datenschutzbeauftragten bestellen, soweit ihre Tätigkeit eine umfangreiche, systematische und regelmäßige Beobachtung von betroffenen Personen erfordert. Auch eine Verarbeitung zum Beispiel von besonders sensiblen Daten (etwa Gesundheitsdaten) nach Artikel 9 Abs.1 DS-GVO oder Daten über strafrechtliche Verurteilungen oder Straftaten nach Artikel 10 Abs. 1 DS-GVO bedarf eines Datenschutzbeauftragten. Das heißt für Unternehmen in Deutschland: Es wird sich voraussichtlich nichts ändern an den bisherigen Voraussetzungen, unter denen ein Datenschutzbeauftragter zu bestellen ist. Wichtig ist aber, die neue Pflicht des Datenschutzbeauftragten über die Einhaltung der DS-GVO zu wachen. Damit entsteht auch für die Unternehmen ein spürbar höheres Haftungsrisiko.

**Welche Konsequenzen drohen bei Verstößen ?**

Bei Verstößen gegen die Verordnung müssen Unternehmen mit sehr erheblichen Bußgeldern rechnen: Diese können sich auf bis zu 20 Millionen Euro oder im Falle eines Unternehmens auf bis zu vier Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs belaufen, je nachdem, welcher der Beträge höher ist.

**Was bedeutet die DS-GVO für ERP Dienstleister und –Anwender?**

Jedes Unternehmen treffen nach der DSGVO erhöhte Dokumentations- und Nachweispflichten. Das bedeutet zunächst, dass Verfahren inkl. der Datenflüsse, die sich innerhalb eines ERP-Systems abspielen, dokumentiert werden müssen. Das Unternehmen muss also insbesondere wissen und festhalten, welche einzelne Verfahren, welche personenbezogen Daten verarbeiten und wohin diese eventuell weitergeleitet werden.

Bedient sich ein Unternehmen eines ERP-Dienstleisters, so ist er darauf angewiesen, dass er entsprechende Informationen von diesem erhält. Dies ist insbesondere dann der Fall, wenn eine Auftragsdatenverarbeitung vorliegt, der ERP-Dienstleister also die Daten auf Weisung des Unternehmens verarbeitet. Das ist typisch dann der Fall, wenn das ERP-System dezentral auf den Servern des ERP-Dienstleisters gespeichert ist und das Unternehmen auf dieses, zum Beispiel über das Internet zugreift.

Deswegen muss der ERP-Anbieter nicht nur einen Überblick über die Verfahren haben, sondern selbst Verzeichnisse über die Verfahren führen und dem Unternehmen zur Verfügung stellen. Diese Verfahrensverzeichnisse muss das Unternehmen vorhalten und auf Anfrage der Datenschutzbehörde vorlegen können.

Daher ist bei der Auswahl eines ERP- Anbieters auch darauf zu achten, dass dieser diesen datenschutzrechtlichen Anforderungen gerecht werden kann. Bei den ERP-Anbietern, bei denen eine Auftragsdatenverarbeitung vorliegt, sind zusätzlich folgende Anforderungen zu beachten:

Das Unternehmen muss mit dem ERP-Dienstleister eine Vereinbarung zur Auftragsdatenverarbeitung schließen. Nach der DSGVO sind weitere Anforderungen an diesen Vertrag gestellt. Deswegen sollte der ERP-Anbieter eine der DSGVO-konforme Vereinbarung zur Verfügung stellen bzw. diese spätestens ab dem 25.05.2018 anpassen.

Viele ERP-Anbieter bedienen sich selbst Unterauftragnehmer, weil sie nicht alle Dienstleistungen selbst anbieten können. In diesem Zusammenhang ist es wichtig, dass alle Dienstleister transparent benannt sind und entsprechende Regelungen getroffen sind.

Weiterhin muss im Rahmen einer Auftragsdatenverarbeitung das Unternehmen Kontrollen bei seinen Dienstleistern durchführen. Viele ERP-Anbieter sind abgeneigt, Fragebögen oder gar eine Kontrolle vor Ort anzubieten, weshalb das Unternehmen seiner Pflicht nicht nachkommen kann. In diesem Zusammenhang ist auch sicherzustellen, dass die Kontrollen auch bei den Unterauftragnehmern stattfinden. Denn was nutzt es dem Unternehmen, wenn zwar der ERP-Dienstleister DSGVO-konform ist, sein Subunternehmer in einem Drittland aber unzureichende Passwörter nutzt. Es muss deswegen gewährleistet sein, dass auch bei den Subunternehmen ein vergleichbares Schutzniveau vorliegt und zumindest der ERP-Dienstleister seine Subunternehmen ausreichend kontrolliert.

Hinsichtlich der Funktionalitäten eines ERP-Systems sind nun die folgenden zwei Prinzipien zu beachten:

Zum einen gilt das Prinzip "privacy by design". Demnach müssen ERP-Anbieter Datenschutz und Datensicherheit bereits in der Planung und Entwicklung ihrer Systeme berücksichtigen. Damit soll sichergestellt werden, dass datenschutzkonforme Funktionalitäten standardmäßig implementiert sind und nicht erst durch nachträgliche und meist umfangreiche Nachprogrammierungen nachgeholt werden müssen. Hierzu gehört die Berücksichtigung von Pseudonymisierung oder Anonymisierung, Aktivierung und Deaktivierung von Funktionalitäten, Absicherungen durch Verschlüsselungen oder Einsatz von Hashfunktionen, Datenminimierung, Authentisierungen, Protokollierung, Zugriffsberechtigungen, Reporting-Funktionen usw.

Zum anderen regelt die DSGVO das Prinzip "data protection by default". Gemeint sind damit datenschutzfreundliche Voreinstellungen von ERP-Systemen. Dadurch sollen nur solche personenbezogene Daten verarbeitet werden, die für die Erfüllung des Zwecks erforderlich sind. Deswegen dürfen z.B. unbemerkt keine Daten ausgewertet und an den ERP-Hersteller (z.B. zu Analysezwecken) übermittelt werden. Möchte der Nutzer trotzdem, dass seine Daten z.B. zu Marketingzwecken ausgewertet und übermittelt werden, muss er dies selbst einstellen. Es soll aber nicht voreingestellt sein, deswegen gilt „data protection by default“.

Eine wichtige Regelung findet sich im Zusammenhang mit der Datensicherheit. Nun muss der ERP-Anbieter und das Unternehmen eine Schutzbedarfs- und Risikoanalyse durchführen und pflegen. Damit das Unternehmen diesen Anforderungen gerecht wird, ist er oft auf die Informationen des ERP-Anbieters angewiesen. Anhand der Risikoanalyse- und Bewertung des ERP-Anbieters kann sich das Unternehmen selbst ein Bild darüber machen, welche Risiken und Schutzmaßnahmen vorhanden sind. Zudem ist gefordert, dass ein Notfallmanagement vorgehalten wird, um die Verfügbarkeit der Daten zu gewährleisten.

In jedem Fall sollte darauf geachtet werden, dass nicht nur einzelne Module wie das HR-Modul von den Regelungen betroffen sind, sondern alle Komponenten, die personenbezogene Daten verarbeiten wie z.B. das CRM-Modul.

Schließlich ist das Unternehmen bei Etablierung und Durchführung von wichtigen Prozessen auf die Mithilfe des ERP-Anbieters angewiesen. Dazu gehören z.B. Prozesse im Zusammenhang mit:

- Anfragen und Ansprüchen Betroffener
- Meldepflicht bei Datenschutzverletzungen
- Überprüfung der ergriffenen Datensicherheitsmaßnahmen

**LKC Jordan GmbH & CO. KG**

Die LKC-Gruppe ist Mitglied von HLB Deutschland und berät an 19 Standorten in Bayern, unter anderem in München und Nürnberg, aber auch in Berlin und Stuttgart in allen Fragen der Wirtschaftsprüfung sowie der Steuer- und Rechtsberatung. Sie beschäftigt rund 400 Mitarbeiter, davon mehr als 75 Berufsträger, und bietet Full-Service für Unternehmer, Unternehmen, Freiberufler, aber auch für Stiftungen, Vereine und Kommunen an. Die LKC-Gruppe gehört damit bundesweit zu den 20 führenden Gesellschaften der Steuerberatungs- und Wirtschaftsprüferbranche. Weitere Informationen unter www.lkc.de.

**HLB Deutschland GmbH**

HLB Deutschland ist ein 1972 gegründetes Netzwerk von 20 selbstständigen und unabhängigen Wirtschaftsprüfungs- und Steuerberatungsgesellschaften an 34 Standorten. Aktuell sind 197 Partner und 1.312 Berufsträger und Mitarbeiter unter dem Dach der HLB Deutschland für die meist mittelständischen Mandanten in Wirtschafts- und Steuerfragen tätig. HLB Deutschland gehört mit einem Gesamtumsatz der einzelnen Mitglieder von 173 Millionen Euro im Jahr 2015 zu den Top 3 der in Deutschland tätigen Netzwerke. HLB Deutschland ist unabhängiges Mitglied von HLB International. Weitere Informationen unter www.hlb-deutschland.de.