EU-DSGVO-Anforderungen mit ELO erfolgreich meistern

Liebe Leser,

am 25. Mai ist die neue Europäische Datenschutz-Grundverordnung (EU-DSGVO) in Kraft getreten – verpflichtend für jedes Unternehmen, ob groß oder klein.

Für die einen ist es eine längst überfällige Maßnahme, um die Menschen im digitalen Zeitalter vor Fake-News und Datenmissbrauch zu schützen. Für die anderen stellt sie eine völlig überzogene Monsterverordnung dar, die gerade kleine und mittlere Unternehmen bei der Umsetzung vor enorme Herausforderungen stellt.

Keine Frage, Datenschutz ist wichtig und dass diesbezüglich nicht selten nachlässig gehandelt wird, weiß jeder. Die Vielzahl an Datenskandalen in den vergangenen Jahren verdeutlicht dies nur allzu gut. Bei kaum einer neuen Verordnung gab es jedoch so viel Verunsicherung wie bei der nun in Kraft getretenen EU-Datenschutz-Grundverordnung.

Dies hängt zum einen sicherlich mit den theoretisch hohen Bußgeldern von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes zusammen. Zum anderen sind aber auch einige Auslegungsschwierigkeiten und der mangelnde Praxisbezug Ursache für die Verunsicherung.

Hierzu lassen sich beispielhaft die Artikel 13 und 14 anführen, welche die vollumfängliche Informationspflicht vor der Erhebung von personenbezogenen Daten regeln. Ein in der Praxis nicht überall realisierbarer Aufwand, der so manchen zur Verzweiflung bringen dürfte.

Ich selbst habe eine Vielzahl an Vorträgen und Workshops zur EU-DSGVO von IT-Juristen und Datenschützern besucht, an deren Ende die Teilnehmer noch verunsicherter waren als zuvor. Dies, weil in den meisten Fällen vor allem eine praxisorientierte Umsetzungsempfehlung fehlte.

An dieser Stelle muss ich dennoch eine Lanze für die einzelnen Datenschutzbehörden der Bundesländer brechen, die trotz Personalknappheit eine hervorragende Arbeit leisten. Sei es durch verständliche Erläuterungen oder praxisorientierte Formulare und wertvolle Tipps.

In der vorliegenden Broschüre wollen wir Sie nicht nur praxisorientiert und kompakt über die wichtigsten Anforderungen der neuen EU-Datenschutz-Grundverordnung informieren: Wir wollen gleichzeitig konkret aufzeigen, wie Sie **ELO for DSGVO** funktional und IT-technisch unterstützt, damit Sie die EU-DSGVO-Anforderungen erfolgreich meistern können.

In diesem Sinne wünsche ich Ihnen viel Erkenntnis und Nutzen beim Lesen!

Karl Heinz Mosbach
Geschäftsführer ELO Digital Office GmbH

Inhalt

> Der Inhalt der Broschüre stellt keine juristische Beratung dar und schließt daher Haftungsansprüche aus. Detailhinweise und Anforderungen sind ggf. durch eine zusätzliche juristische Beratung auf die eigenen Unternehmensanforderungen zu überprüfen.

EU-DSGVO im Überblick

EU-DSGVO: Die Verantwortung liegt beim Geschäftsführer

Auch wenn das Thema Datenschutz in hohem Maße vor allem den IT-Verantwortlichen und den Datenschutzbeauftragten betrifft, trägt beim Thema EU-DSGVO die Geschäftsführung die Verantwortung. Sie muss veranlassen, dass die notwendigen Maßnahmen im Unternehmen umgesetzt werden.

Hieraus ergibt sich ein (persönliches) Haftungsrisiko, zum einen wegen der möglichen hohen Bußgelder, die durch die Aufsichtsbehörde verhängt werden können. Zum anderen, da Mitarbeiter im Falle von Versäumnissen und gravierenden Verletzungen der EU-DSGVO das Unternehmen auf immateriellen Schadensersatz verklagen können.

› **Daher:**
Datenschutz ist Chefsache!
Die nötigen Maßnahmen anzuordnen ist ein Leichtes, diese zu ignorieren ist grob fahrlässig.

Bußgelder und Haftungsrisiken

Auch wenn mit Inkrafttreten der EU-DSGVO nicht gleich mit einer Welle von hohen Bußgeldverfahren zu rechnen ist, so sind die Risiken – insbesondere bei groben Verstößen – dennoch gegeben. Dies unterstreicht der hohe Bußgeldrahmen von bis zu 4 % des weltweiten Jahresumsatzes sowie die Meldepflicht an die zuständige Aufsichtsbehörde bei einer Datenpanne binnen 72 Stunden.

So wäre im Falle von Facebook und des gravierenden Datenskandals mit Cambridge Analytica ein möglicher Bußgeldrahmen von bis zu 1,6 Mrd. $ gegeben gewesen. Dieses Beispiel veranschaulicht den weitreichenden Handlungsspielraum der Datenschutzaufsichtsbehörden, die – am Rande bemerkt – auch unangekündigte Kontrollen durchführen dürfen. Wie es dann in der Praxis kommen wird, wird man in nächster Zeit sehen. Bei Nichteinhaltung besteht für Unternehmen aber immer das folgende Risiko: Man kann vom Wettbewerb abgemahnt oder von Betroffenen, wie ehemaligen Mitarbeitern oder verärgerten Kunden, auf immateriellen Schaden verklagt werden.

Auch wenn zu hoffen bleibt, dass sich diese Fälle in Grenzen halten, ist auch mit dem Gegenteil zu rechnen – schließlich eröffnen sich hier einige neue Möglichkeiten für spezialisierte Abmahnkanzleien.

Allein schon deshalb sollten die notwendigen Maßnahmen zur Einhaltung der EU-DSGVO umgesetzt sein.

Wann dürfen personenbezogene Daten verarbeitet werden?

Prinzipiell dürfen personenbezogene Daten nicht verarbeitet werden – außer, es liegt ein sogenannter Erlaubnistatbestand vor.
Dies ist der Fall, wenn …

1. … eine Person explizit und freiwillig der Verarbeitung ihrer Daten zugestimmt hat.

Dies kann durch Unterschrift auf einem Formular oder durch einfaches Anklicken einer Einverständniserklärung (Opt-In) im Internet geschehen. Wichtig dabei ist, dass die einwilligende Person klar über Form und Zweck der Datenerfassung/-verarbeitung informiert (Datenschutzrichtlinie) und darauf hingewiesen wird, dass die Einwilligung jederzeit widerrufen werden kann.

Bei einer Newsletter-Registrierung ist darauf zu achten, dass die Korrektheit der E-Mail-Adresse durch das Double-Opt-In-Verfahren (zusätzliche Bestätigungs-E-Mail) bestätigt wird. Zum Nachweis sollten Name, Datum, Zeit und IP-Adresse (bzw. Ort) im System protokolliert sein. Gleiches gilt für Visitenkarten, wenn diese in einer Adressdatenbank/Kartei erfasst werden.

> **Hinweis:**
> Für eine bestehende Kontaktdatenbank müssen keine erneuten Einverständniserklärungen eingeholt werden, wenn diese vor der EU-DSGVO nach dem damals gültigen Recht (95/46/EG) erhoben wurden.

2. … die Daten aus Gründen der Erfüllung einer vertraglichen Verpflichtung gespeichert und verarbeitet werden müssen.

Dies ist natürlich in jeder Kundenbeziehung gegeben. Wichtig dabei ist, dass die Daten nur zweckgebunden verarbeitet werden dürfen. Eine Weitergabe der Daten an Dritte ohne eine explizite Einverständniserklärung ist grundsätzlich nicht gestattet. Ist die Weitergabe von personenbezogenen Daten (z. B. an eine Spedition) zur Vertragserfüllung erforderlich, ist dies natürlich erlaubt. Hierzu bedarf es aber eines klaren Hinweises in den Datenschutzbestimmungen. Zusätzlich sei darauf verwiesen, dass mit allen Unternehmen, die Daten im Auftrag eines Verantwortlichen verarbeiten, eine schriftliche Vereinbarung zur Datenweiterverarbeitung abgeschlossen werden muss. Im Falle der Auftragsverarbeitung (z. B. Cloud-Dienste, externe Dienstleister, Shop-Anbieter usw.) sind beide Seiten in der Verantwortung.

3. … es um die Wahrung berechtigter Interessen des Verantwortlichen geht.

Demnach dürfen personenbezogene Daten von Unternehmen verarbeitet werden (z. B. Direktmailings zu neuen Produkten, Kundenauswertungen usw.) sofern nicht die Interessen der betroffenen Personen überwiegen, die den Schutz personenbezogener Daten erfordern. Zudem gilt natürlich die Einhaltung der Betroffenenrechte. In diesem Zusammenhang sei erwähnt, dass es auch erlaubt ist, weitere Daten zweckgebunden zu erheben und auszuwerten, um beispielsweise einen Kunden richtig beraten zu können. Bei der Erhebung und Speicherung solcher Daten bedarf es also keiner zusätzlichen Einverständniserklärung.

4. Wichtig in allen Fällen: die Informationspflicht!

Werden personenbezogene Daten erfasst, müssen die Betroffenen vorab immer ausführlich über die entsprechende gültige Firmen-Datenschutzrichtlinie informiert werden (Art. 13/Art. 14). Was sich auf den Internetseiten noch sehr einfach realisieren lässt, kann im Alltag – beispielsweise bei einer Terminvereinbarung bei einem neuen Zahnarzt per Telefon – schnell zum Problem werden. In diesem Falle sieht es das ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) für ausreichend an, wenn die Datenschutzbestimmungen klar ersichtlich auf der Homepage der Praxis dargestellt sind und beim ersten Besuch ein Informationsblatt zu den Datenschutzbestimmungen ausgehändigt wird. Generell darf aber festgestellt werden, dass im Falle von Art. 13/Art. 14 definitiv noch Klärungsbedarf besteht.

5. Weitere Fälle

Der Vollständigkeit halber sei erwähnt, dass der Erlaubnistatbestand auch vorliegt bei:

- Erfüllung rechtlicher Verpflichtungen
- Schutz von lebenswichtigen Interessen betroffener Personen
- Wahrung einer Aufgabe im öffentlichen Interesse

- **Hinweis zur Auftragsverarbeitungsvereinbarung (AVV):**
  Werden personenbezogene Daten zur Verarbeitung an Dritte weitergegeben, ist eine schriftliche AVV abzuschließen. Bei beiläufiger Kenntnisnahme von Daten (Transport-Dienstleistung, Support/Wartung) ist keine AVV nötig. Obwohl es sich um eine vertragliche Vereinbarung handelt, genügt es diese in elektronischer Form (gescannt oder als PDF-Dokument) aufzubewahren.

Im Falle von personenbezogenen Daten, die sich auf eine identifizierte oder identifizierbare, natürliche Person beziehen, unterscheidet die EU-DSGVO zwei Kategorien:

a) Allgemeine Daten wie Kontaktdaten (Name, Adresse, Telefon, E-Mail- und IP-Adresse usw.)
b) Persönliche, sensible Daten der besonderen Kategorie (wie Religion, Erkrankungen, biometrische Daten usw.). Diese Daten weist die EU-DSGVO als besonders schützenswerte Daten aus.

Betroffenenrechte wahren

Eine echte Herausforderung für viele Unternehmen ist die Wahrung der – mit der EU-DSGVO erheblich gestärkten – Betroffenenrechte. Diese umfassen im Wesentlichen:

1. Auskunftsrecht

Jeder Betroffene hat durch die EU-DSGVO das Recht, binnen eines Monats Auskunft zu erhalten, welche personenbezogenen Daten über ihn gespeichert sind. Oft fehlen in Unternehmen der Überblick und Werkzeuge, um auf diese Anfrage schnell Auskunft geben zu können. Hier muss durch die technischen und organisatorischen Maßnahmen (TOMs) sowie entsprechende Prozesse Abhilfe geschaffen werden. In jedem Fall muss vor der Herausgabe von Daten sichergestellt sein, dass es sich beim Antragsteller auch um die richtige Person handelt.

2. Recht auf Übertragung eigener Daten

Jeder Betroffene hat das Recht zu verlangen, dass seine Daten übermittelt und ihm zur Verfügung gestellt werden. Solange es hierbei nur um reine Kontaktdaten geht, ist dies sicherlich kein Problem. Wenn es sich aber um umfangreiche Kunden-, Patienten-, Bauakten und den E-Mail-Verkehr handelt, wird es schwierig: Ohne technische Unterstützung ist der manuelle Aufwand hoch, die Kosten sind entsprechend intensiv. Werden Daten übertragen, z. B. in einer ZIP-Datei oder auf einem Datenträger, ist darauf zu achten, dass diese verschlüsselt sind und das Passwort separat (z. B. per SMS oder Brief) übermittelt wird.

3. Recht auf Löschung

Prinzipiell hat jeder Betroffene das Recht, die Löschung seiner Daten zu verlangen, sofern gesetzliche Aufbewahrungsfristen oder sonstige Regeln nicht dagegensprechen. So müssen z. B. kaufmännische Belege aus steuerrechtlichen Gründen zehn Jahre aufbewahrt werden – hier wird die EU-DSGVO also von einem anderen Gesetz überlagert. Ist ein Löschen für aufbewahrungspflichtige Informationen technisch nicht möglich (z. B. Bandsicherung), ist der Zugriff darauf einzuschränken bzw. zu sperren.

In vielen Fällen schreiben die gesetzlichen Vorgaben sogar explizit das Löschen von Daten in vorgegebenen Zeiträumen vor, sofern keine persönliche Einwilligungserklärung vorliegt. Bewerbungsunterlagen müssen in der Regel nach drei Monaten gelöscht werden. Eine in diesem Zusammenhang erstattete Reisekostenabrechnung allerdings nicht. Diese muss wiederum aus steuerrechtlichen Gründen zehn Jahre aufbewahrt werden. Schaut man sich die gängige Unternehmenspraxis an, so wurde eine gezielte Datenlöschung bisher nur wenig vorangetrieben. Zu aufwendig und zu teuer schien das Unterfangen. Als Folge horten viele Unternehmen Unmengen an Uraltdaten, die keine rechtliche und inhaltliche Relevanz mehr haben. Dies ist mit Inkrafttreten der EU-DSGVO nicht mehr möglich. Hier sind Lösungen zu implementieren, die mit Ablauf der Aufbewahrungsfristen personenbezogene Daten nachvollziehbar und protokolliert löschen (Art. 19). Weitere Rechte bestehen bezüglich der Berichtigung, der Informationspflicht und des Widerspruchsrechts.

Weitere Betroffenenrechte sind:

- **Recht auf Berichtigung**
- **Informationspflicht**
- **Widerspruchsrecht**
- **Recht auf Einschränkung**

Maßnahmen zur IT-Sicherheit

Die IT-Sicherheit zu gewährleisten ist sicherlich nicht erst seit der neuen EU-DSGVO ein wichtiger Aspekt für Unternehmen. Die Rahmenbedingungen zur IT-Sicherheit gibt es schon lange, sie bekommen aber mit den möglichen hohen Bußgeldern (z. B. bei einer Datenpanne) einen anderen Stellenwert. So ist die Umsetzung von geeigneten IT-technischen und organisatorischen Maßnahmen (TOMs) Pflicht. Gerade in kleinen und mittleren Unternehmen sind hier vereinzelt noch gravierende Defizite zu verzeichnen. Sei es durch veraltete Firewalls oder aber Backups, die keine History haben und einfach überschrieben werden können. Hinzu kommen teils offene Datenzugriffe oder Serverräume, die zum Materiallager zweckentfremdet wurden und deshalb für alle Mitarbeiter frei zugänglich sind.

Die Beispiele hierfür sind mehr als zahlreich. Mit Einführung der EU-DSGVO erhalten solche Nachlässigkeiten eine besondere Brisanz. Es empfiehlt sich, die IT-Sicherheit Stück für Stück zu überprüfen und zu dokumentieren. Auch ein Audit durch einen externen Sachverständigen ist im Grunde ratsam. Checklisten und Ratgeber gibt es hierzu genügend. Diese Maßnahmen sind in jedem Fall als unbedingt notwendig zu erachten, denn Datendiebstahl oder Datenverlust können einen weitaus größeren finanziellen Schaden verursachen.

Verpflichtung zur Dokumentation

Fast jedes Unternehmen ist in der Pflicht, ein Verzeichnis der Verarbeitungstätigkeiten gemäß EU-DSGVO (Art. 30) zu erstellen. Dieses Verzeichnis dokumentiert, in welchen Bereichen und Systemen (Applikationen, Datenbanken usw.) personenbezogene Daten verarbeitet werden. Hinzu kommt die Dokumentation über die technischen und organisatorischen Maßnahmen (TOMs), die man zur Einhaltung und Gewährleistung der Datenschutzbestimmungen ergriffen hat.

Viele, gerade auch kleinere Unternehmen, schreckt der womöglich große Arbeitsaufwand ab. Natürlich wird für die Erstellung Zeit benötigt – geht man dies gemeinsam und strukturiert an, kann es aber auch schnell erledigt sein. Insbesondere, da alle Aufsichtsbehörden hervorragende Musterformulare (z. B. für das Verzeichnis der Verarbeitungstätigkeiten) zur Verfügung stellen. Das Gleiche gilt für die TOMs, für die ebenfalls Checklisten und Formulare zur Verfügung gestellt werden. Aufgeteilt auf die einzelnen Bereiche und Personen ist der Aufwand dann durchaus überschaubar. Neben der Erfüllung der EU-DSGVO-Anforderungen hat die Dokumentation für das Unternehmen einen weiteren Vorteil**:** Der Datenschutz wird transparent und nachvollziehbar – egal, ob es sich um personenbezogene oder unternehmenssensible Daten handelt.

Datenschutzfolgeabschätzung

Werden im eher seltenen Falle sehr umfangreiche personenbezogene Daten der besonderen Kategorie (sensible Daten) und neue Technologien eingesetzt, ist eine Datenschutzfolgeabschätzung durchzuführen. Diese ist im Wesentlichen eine Riskobetrachtung/-analyse betreffend der IT-Sicherheit und der Prozesse.

Datenschutzbeauftragter

Die Pflicht, einen Datenschutzbeauftragten zu ernennen, ist in den EU-Ländern unterschiedlich geregelt. In Deutschland benötigen Unternehmen einen Datenschutzbeauftragten, wenn mindestens zehn Mitarbeiter kontinuierlich in ihrer Kerntätigkeit (z. B. Vertrieb, Marketing, Auftragszentrum usw.) personenbezogene Daten verarbeiten. Mitarbeiter, zu deren Hauptaufgabe nicht das Bearbeiten (erfassen, speichern usw.) von personenbezogenen Daten zählt, sondern nur ein gelegentlicher Kontakt damit besteht (z. B. Handwerker, Mechaniker usw.) zählen nicht dazu. Muss ein Datenschutzbeauftragter eingesetzt werden, kann ein Mitarbeiter sich durch Weiterbildung qualifizieren oder ein externer Datenschutzspezialist übernimmt die Aufgabe. Dies ist gerade für kleine Firmen interessant. Der Datenschutzbeauftragte muss der zuständigen Aufsichtsbehörde über deren Webseite gemeldet werden.

Die wichtigsten organisatorischen Maßnahmen im Überblick

- ☑ Verarbeitungstätigkeiten und TOMs dokumentieren
- ☑ Mitarbeiter unterweisen und schulen
- ☑ Unternehmensrichtlinie (z. B. Betriebsvereinbarung) zum Thema Datenschutz und Umgang mit personenbezogenen Daten aufsetzen

  Empfehlung: Hier sollte festgehalten werden, dass private Daten nicht mit Unternehmensdaten vermischt werden dürfen. So sollte beispielsweise das Versenden von privaten E-Mails über den Firmen-E-Mail-Account untersagt sowie der Empfang von privaten E-Mails sofort separiert und gelöscht werden.
- ☑ Nachweis der Einwilligungserklärungen sicherstellen (Protokollierung: Name, Datum, IP-Adresse, Ort usw.)
- ☑ Einen schriftlichen Vertrag mit dem Auftragsverarbeiter (externe Dritte) erstellen
- ☑ Datenschutzrichtlinien insbesondere auf die Informationspflicht und die Betroffenenrechte anpassen
- ☑ Zugriffsberechtigungen, Verschlüsselungen, allgem. Sicherheit überprüfen und optimieren
- ☑ Ggf. Datenschutzbeauftragten benennen und der zuständigen Aufsichtsbehörde melden

Der Umgang mit den Aufsichtsbehörden

Prinzipiell sind die Aufsichtsbehörden nicht nur dafür verantwortlich, Bußgelder zu verhängen, sie beraten gleichermaßen Unternehmen in EU-DSGVO-Fragen. Dennoch verfügen die Behörden über weitreichende Befugnisse, wie z. B. die Durchführung unangemeldeter Kontrollen und Überprüfungen. Überaus wichtig ist, dass Unternehmen Datenpannen (z. B. Datendiebstahl) binnen 72 Stunden der Aufsichtsbehörde melden müssen. Verheimlichen sollte man eine Datenpanne keinesfalls: Gerade in einem solchen Fall ist die Wahrscheinlichkeit sehr hoch, ein hohes Bußgeld zu erhalten.

Die gute Nachricht: ELO for DSGVO

Für alle ELO Benutzer und diejenigen, die es noch werden wollen, gibt es eine gute Nachricht: ELO ist die ideale Plattform zur Umsetzung und Einhaltung der EU-DSGVO-Anforderungen. In der **ELO ECM Suite 11** werden zahlreiche funktionale Details wie Löschfristen, globale personenbezogene Datenfelder, eine Verarbeitungsdatenbank, Standardformulare und vieles mehr bereitgestellt: **ELO for DSGVO** – unsere Funktionalitäten für Ihren Schutz personenbezogener Daten.

Personenbezogene Datenkennung im Standard

Heute sind personenbezogene Daten in sämtlichen Unternehmensbereichen verstreut – sei es in E-Mail-Postkonten, Datenbanken oder in beliebigen File-Verzeichnissen. Möchte ein Betroffener Auskunft über seine gespeicherten personenbezogenen Daten erhalten, entstehen für das Unternehmen nicht nur ein erheblicher Aufwand, sondern auch entsprechende Kosten.

Um dies zu vermeiden, hat ELO ab der Version 11 seiner ECM Suite eine feste Kennung „DSGVO-Bezug" im Datenmodell implementiert. Über diese lässt sich nun vorgangs- und bereichsübergreifend ein eindeutiges Personenmerkmal (Name, ggf. mit Personalnummer, Kundennummer usw.) für jedes Dokument, jede Datei, sämtliche Metadaten usw. mitführen. Per Mausklick ist ersichtlich, welche Daten zu einer Person (Kunde, Interessent usw.) gespeichert worden sind. Sensible Daten (z. B. Personaldaten) sind natürlich nur mit den entsprechenden Zugriffsberechtigungen (Verschlüsselung) einsehbar.

Lösch- und Aufbewahrungskennung

Neu in der **ELO ECM Suite 11** ist auch das globale Merkmalsfeld „Ende Löschfrist". Zusammen mit dem Feld „Ende Aufbewahrungsfrist" steuert dieses einen automatisierten Löschvorgang: Alte oder bedeutungslose Daten können hiermit genauso automatisch gelöscht werden wie Daten, die gemäß EU-DSGVO zu löschen sind. Müsste man dies manuell durchführen, wären Aufwand und Kosten hoch.

Mit ELO verläuft dieser Prozess sicher, automatisiert und protokolliert, so dass immer Transparenz und Auskunftsfähigkeit gegeben sind. Gleichzeitig werden gesetzliche Aufbewahrungsfristen berücksichtigt: Bei kaufmännischen Belegen, die über zehn Jahre aufbewahrt werden müssen, setzt diese Frist ein Löschbegehren solange außer Kraft, bis die Mindestaufbewahrungszeit erreicht ist.

Abbildung zeigt:
DSGVO-Datenfelder in der **ELO ECM Suite 11**