LINDA LIESUM
SACHVERSTÄNDIGE FÜR
WIRTSCHAFTSKRIMINALITÄT
& COMPLIANCE

Im ersten Schritt wurde die Einhaltung der EU-DSGVO vordringlich auf die Anpassung der Datenschutzhinweise im Internet bezogen, um den Informationspflichten nachzukommen

EU-DSGVO, der Tag danach - und alles ist gut?

@wladimir1804 / Fotolia

Die Notwendigkeit für die Einhaltung der Datenschutzrichtlinien ist im Management als solche angekommen, nun gilt es alltägliche Schwachstellen weiter zu eliminieren und für die notwendige Dokumentation und Mitarbeitersensibilisierung zu sorgen.

Die Umsetzung der EU-Datenschutz-Grundverordnung (EU-DSGVO) wurde und wird in Unternehmen mit viel zeitlichem und finanziellem Aufwand betrieben.

Nach Vorstellung des Gesetzgebers soll mit der neuen EU-DSGVO seit dem 25.05.2018 in allen europäischen Ländern durch ein gemeinsames Gesetz ein gleichartig hohes Datenschutzniveau umgesetzt worden sein. Für alle Menschen in Europa soll inzwischen mehr Transparenz und Sicherheit bei der Verarbeitung ihrer personenbezogenen Daten gewährleistet sein.

Nach Ansicht der deutschen Aufsichtsbehörden sollen sich durch die EU-DSGVO Wettbewerbsvorteile für europäische und insbesondere für deutsche Unternehmen ergeben. Aber einstweilen ist nur ein immenser Aufwand entstanden, bei dem insbesondere darauf geachtet wurde, aus der Außensicht erkennbare Datenschutzaspekte, wie Informationspflichten und Datenschutzhinweise für den Internetauftritt, entsprechend der neuen Vorgaben umzusetzen.

Die Rechtsunsicherheit in allen Themen des Datenschutzes ist durch die wenig detaillierten gesetzlichen Vorgaben sehr groß. Rechtsmeinungen zu Vorgaben entstehen erst langsam. In vielen europäischen Staaten wurden noch keine lokalen Ergänzungsgesetze, wie es auch das Bundesdatenschutzgesetz darstellt, in Kraft gesetzt.
Die Beachtung der Öffentlichkeit und der Medien für das Thema „Datenschutz" war und ist so groß wie noch niemals zuvor. Doch hat der Aufwand, der betrieben wurde, tatsächlich eine Verbesserung des Datenschutzniveaus in den Unternehmen bewirkt?

Alltägliche Datenschutz-Schwachstellen annähernd unverändert

Verbesserungen können dahingehend erkannt werden, dass der Datenschutz seitens des Managements wesentlich mehr Beachtung findet als bisher. Deshalb ist auch die Durchsetzbarkeit von Maßnahmen so hoch wie nie zuvor. Dieser Effekt ist nicht nur im Management der Unternehmen vorhanden, sondern aufgrund der großen Verbrei-

tung der Datenschutzthemen in der Presse auch in weiten Teilen der Belegschaften.

Unsere Erfahrungen zeigen, dass es weiterhin Ansatzpunkte gibt, um in Unternehmen ein ausreichendes Datenschutzniveau zu erreichen.

Nachfolgend werden exemplarisch regelmäßig in Unternehmen vorzufindende Missstände im Datenschutzmanagement aufgezeigt.

Fehlende Dokumentationen

Nachweispflichten der Einhaltung des Datenschutzes liegen nun gemäß EU-DSGVO bei jedem Unternehmen (Umkehr der Beweislast). Internen Dokumentationen zum Datenschutz ist ausreichend Beachtung zu schenken. Das nach Art. 30 EU-DSGVO vorgeschriebene Verzeichnis der Verarbeitungstätigkeiten ist Kernpunkt in der Nachweisführung. Darin müssen Angaben zu jeder Verarbeitung vorhanden sein. Damit zusammenhängend sollten Löschkonzepte für die Verfahren bestehen.

Als Schlüsselpunkt für Datenschutzmaßnahmen sind Berechtigungskonzepte erforderlich. Wer in Programmen Eingaben oder Änderungen vornehmen darf, ist Inhalt eines Berechtigungskonzepts. Damit kann nachgewiesen werden, dass die Berechtigungen auf ein notwendiges Mindestmaß beschränkt worden sind und das Prinzip der Vertraulichkeit verfolgt wird.

Die interne Dokumentation zu vorgesehenen Prozessen zum Datenschutz sollte sich in einer Datenschutzrichtlinie widerspiegeln, die gleichzeitig Vorgehensweisen bei Betroffenenanfragen darlegt.

Schließlich rundet ein Notfallkonzept die Dokumentationslage zur geforderten Wiederherstellbarkeit und Verfügbarkeit der Daten ab.

Fehlende vertragliche Vereinbarung

Kaum ein Unternehmen führt die Verarbeitung von personenbezogenen Daten vollständig selbst aus. Dienstleister werden beauftragt, und erhalten z.B. für Werbeanschreiben Datenbestände von Adressdaten. Für solche Auftragsverarbeitungen müssen nach Art. 28 EU-DSGVO schriftliche Verträge geschlossen werden, die ausreichende Inhalte zum Schutz der personenbezogenen Daten haben.

In den Bereich der fehlenden Vereinbarung sind auch die fehlenden Vertraulichkeitserklärungen mit eigenen Mitarbeitern einzuordnen. Auch, wenn der § 5 des alten Bundesdatenschutzgesetzes entfallen ist, der dies ausdrücklich und schriftlich einforderte, so besteht weiterhin die Verpflichtung, Mitarbeiter, welche in ihrer Tätigkeit mit personenbezogenen Daten umgehen, zur Vertraulichkeit zu verpflichten. Dies ist auch bei Eintritt in ein Unternehmen ein erster Ansatzpunkt zur Datenschutz-Sensibilisierung von Mitarbeitern.
Weiterhin empfiehlt sich mit Mitarbeitern die rein betriebliche Nutzung von Internet und E-Mail am Arbeitsplatz zu vereinbaren. Abgrenzungsprobleme zur Privatsphäre des Mitarbeiters und datenschutzrechtliche Fragen können somit besser gehandhabt werden.

Zur Erinnerung: Die Erweiterung der Haftung auf den gesamten Konzern für Verstöße gegen die DSGVO kann Bußgelder bis 20 Mio. EUR bzw. Geldstrafen bis zu 4 % des weltweit erzielten Umsatzes betragen.

Linda Liesum

Sachverständige für Wirtschaftskriminalität und Compliance

DIN EN ISO/iEC 17024 zertifizierte Sachverständige für Wirtschaftskriminaität und Compliance der Akkreditierungsstelle des European Committee for Quality Assurance GEIE in Brüssel Zertifizierungsnr. 1-16-1041

Tel.-Nr. 06126 9513 343
linda.liesum@forensic-sv.de

Wiesbadener Str. 7
65510 Idstein

Fehlende technische Absicherung

Einfache technische Maßnahmen sind oft sehr wirkungsvoll zum Datenschutz: eine automatische Bildschirmsperre schützt vor ungewollter Bildschirmeinsicht oder IT-Nutzung, wenn sich der Benutzer auch nur kurzzeitig vom Arbeitsplatz entfernt.

Kombiniert mit einer Passwortwechselroutine (erzwungener Wechsel,

Passworthistorie, Sperrung nach mehrmaligen Fehlversuchen) entstehen wirkungsvolle Schutzschranken. Datenschutz ist nicht immer bequem, Sicherheitsmaßnahmen i.d.R. auch nicht, aber so ist auch die Nutzung eines Sicherheitsgurts im Fahrzeug schnell von „unbequem" zur akzeptierten Maßnahme zum Schutz der Fahrzeuginsassen geworden.

Auch kann ein Berechtigungskonzept seine Wirkung nicht entfalten, wenn Nutzer mit ihren Passworten nicht vertraulich umgehen.

Natürlich sind in jedem Fall auch weitere administrative Maßnahmen empfehlenswert: Umfangreiche administrative Rechte von Endbenutzern auf Endgeräten und unverschlossene USB-Ports sind einfache Einfallstore für jegliche Schadsoftware. Es ist hier nicht unbedingt zwischen Datenschutz- und Informationssicherheitsmaßnahmen zu unterscheiden, wichtig ist die Wirksamkeit für den Schutz der personenbezogenen Daten.

Zum Standard sollte auch gehören, dass zentrale IT-Komponenten, insbesondere Server, Router, Switches, in einem gesonderten, klimatisierten Raum aufgestellt sind. Schließlich dürften hier im Normalfall alle verarbeiteten Daten kumuliert zusammenlaufen und Ausfälle haben i.d.R. direkt große Wirkung. Auch wenn Platznot im Unternehmen besteht, sollte ein Serverraum nicht Abstellraum für Putzmittel oder Akten sein. Sowohl technikfremde Personen wie auch die Einbringung von zusätzlichen Brandlasten sind der Sicherheit abträglich.

Fehlende Mitarbeitersensibilisierung

Wie zu allen Zeiten ist der Mensch die Schaltstelle für alles was im Unternehmen stattfindet. Seine Aufmerksamkeit sowie sein Umgang entscheiden darüber, ob Datenschutz im Unternehmen „gelebt" wird. Deshalb ist es wichtig nicht an der Schulung und Sensibilisierung der Mitarbeiter zu sparen. Dabei geht es nicht um das Durchlaufen von mehrtätigen Schulungsprogrammen. Wichtig ist, jeden Mitarbeiter im Kontext seiner Arbeitssituation auf die Problemstellen im Umgang mit personenbezogenen Daten aufmerksam zu machen.

Dazu gehört weiterhin z.B. die richtige „Aufbewahrung" von Passwörtern. Für Mitarbeiter an der Telefonzentrale ist der sensible Umgang bei telefonischen Anfragen zu Kunden- und Mitarbeiterinformationen relevant. Mitarbeiter im Außendienst müssen bei betrieblichen Telefonaten darauf achten, in unsicheren Umgebungen keine sensiblen Informationen mitzuteilen (im Zug, im Flughafen). Auch die sichere Aufbewahrung eines Notebooks ist eine einfache Möglichkeit „datenschützend" zu wirken.

Datenschutz: es bleibt viel zu tun!

Auch wenn die EU-DSGVO den Datenschutz in der Wahrnehmung sämtlicher Marktteilnehmer nun hervorgehoben hat, es bleibt viel zu tun, wenn das Gesetz zur Verbesserung des Datenschutzniveaus in den Unternehmen nachhaltig beitragen soll. Die Umsetzung von Informationspflichten zur verbesserten Transparenz für die Betroffenen ist wenig hilfreich, wenn in den Unternehmen weiterhin viele Lücken in den Datenschutzmaßnahmen bestehen.

Da aufgrund der Beweislastumkehr nun jedes Unternehmen mehr als bisher gefordert ist, Datenschutzmaßnahmen nachweisen zu müssen, sollten Unternehmensleitungen die zur EU-DSGVO begonnenen Projekte und Aktivitäten dahingehend nutzen, auch die praktische Umsetzung und Wirkung der implementierten Datenschutzmaßnahmen auf den Prüfstand zu stellen. Schließlich werden einsetzende Kontrollen der Datenschutz-Aufsicht nicht nur auf die Umsetzung der Transparenzpflichten beschränkt sein.

Die Verantwortung für den umfassenden Datenschutz ist und bleibt in den Händen der Unternehmensführung. Diese Verantwortung nicht ausreichend wahrzunehmen, kann Unternehmen aufgrund der neuen Strafvorschriften sehr teuer zu stehen kommen.

Zusammenfassung

Seit dem 25.05.2018 gilt die neue EU-Datenschutzgrundverordnung (DSGVO)

Nutzen Sie die aktuelle Bereitschaft des Managements, um jetzt die nächsten Schritte umzusetzen:

- Fehlende Dokumentation eliminieren: Das nach Art. 30 EU-DSGVO vorgeschriebene Verzeichnis der Verarbeitungstätigkeiten ist Kernpunkt in der Nachweisführung.
- Implementierung einer Datenschutzrichtlinie verbunden mit einem Löschkonzept.
- Vertragliche Vereinbarungen mit Fremdleistern aufsetzen
- Technische Absicherungen (IT) einführen
- Durchführung von Mitarbeiter-Schulungen für „gelebten Datenschutz"

Die Verantwortung für die Einhaltung von datenschutzrechtlichen Maßnahmen obliegt der Unternehmensführung. Dennoch kann jeder Einzelne dazu beitragen, dass Datenschutz gelebt wird, wenn er die generelle Faustregel beachtet: Die Daten von anderen sind so zu behandeln, wie man seine eigenen Daten behandelt wissen möchte.