Neue Aufgaben für (HR-) Fach- und Führungskräfte

durch die Datenschutz-Grundverordnung

Die Reform des europäischen Datenschutzrechtes wirkt sich auf alle Bereiche und Abteilungen eines Unternehmens aus. Der Personalbereich ist davon besonders betroffen, da hier eine Vielzahl von Daten zu verschiedenen Zwecken verarbeitet wird. Die Einhaltung des neuen Datenschutzrechtes kann nicht mehr allein dem Datenschutzbeauftragten oder der Rechtsabteilung überlassen werden. Vielmehr sind auch Führungskräfte und der Personalbereich in der Verantwortung, die neuen Vorgaben und Anforderungen umzusetzen. Dies fängt mit dem Beschaffungsprozess von Produkten und Dienstleistungen an, geht über die Verarbeitung von Daten und die Zusammenarbeit mit dem Betriebsrat und endet bei der Löschung von Daten. Aufgrund einer Beweislastumkehr muss dabei für jeden einzelnen Schritt die Datenschutzkonformität jederzeit nachweisbar sein.

1 Einleitung

In der letzten Ausgabe der LOHN+GEHALT hatte ich an dieser Stelle das neue europäische Datenschutzgesetz, die Datenschutz-Grundverordnung (DS-GVO), kurz vorgestellt. Inzwischen wurde die DS-GVO am 04.05.2016 im Amtsblatt der EU (L119) veröffentlicht. Wirksam wird das neue Gesetz nach einer zweijährigen Übergangszeit am 25.05.2018. Angesichts der zahlreichen neuen Anforderungen, die auf Unternehmen zukommen, ist dies ein knapp bemessener Zeitraum. In dieser Ausgabe beschäftige ich mich näher mit den konkreten Auswirkungen für HR-Führungskräfte.

2 Erweiterung des Aufgabenspektrums

Datenschutz hat seit jeher einen hohen Stellenwert im Personalbereich. Mit der DS-GVO erwächst jedoch die Notwendigkeit, die Verantwortung für die Einhaltung von Datenschutzvorschriften stärker im betrieblichen Alltag auf allen Hierarchie-Ebenen zu verankern. Auf Führungskräfte im Personalbereich kommt die Aufgabe zu, mit Unterstützung des Datenschutzbeauftragten oder externer Datenschutzberater die Vorgaben der DS-GVO auf die Abläufe im Personalbereich herunterzubrechen und in Prozessen und Softwareanwendungen zu verankern.

Die DS-GVO verlangt unter dem Stichwort „Rechenschaftspflicht", dass ein Unternehmen jederzeit belegen können muss, dass es die Vorschriften der DS-GVO vollständig einhält.[1] Bei der Einführung neuer Abläufe oder der Änderung bestehender Abläufe treten unter bestimmten Bedingungen die Pflicht zur Datenschutz-Folgeabschätzung[2] und die Pflicht zur vorherigen Konsultation der Datenschutzaufsichtsbehörde[3] hinzu. Auch unterhalb der Schwelle zur Datenschutz-Folgeabschätzung definiert die DS-GVO verbindliche Vorgaben, wie in Prozessen personenbezogene Daten verarbeitet werden dürfen (siehe Abschnitt 3). Ebenso gelten für den Einkauf von Softwareprodukten und Dienstleistungen neue Anforderungen (siehe Abschnitt 4).

Die neuen Vorgaben der DS-GVO stehen in einer engeren Wechselwirkung als bisher im Bundesdatenschutzgesetz (BDSG) vorgesehen.

Beispiel:

Ein Geschäftsführer fordert eine Auswertung zur Qualifikationsverteilung in der Belegschaft an. Es muss geprüft und belegt werden, aufgrund welcher gesetzlichen Erlaubnis (Einwilligung, Vertragserfüllung oder Rechtsvorschrift) die Erstellung erlaubt ist. Bei der Erstellung der Auswertung ist technisch oder organisatorisch sicherzustellen, dass nur auf die für die Auswertung relevanten Daten zugegriffen wird. Es kommt dabei nicht allein auf das Ergebnis an, sondern auf jeden einzelnen Verarbeitungsschritt. Weiterhin ist zu prüfen, ob die Belegschaft über die Auswertung zu informieren ist. Dies ist regelmäßig der Fall, sofern der Zweck in einer früheren Information nicht genannt wurde.

Wenn für die Erstellung personenbezogene Daten verwendet werden, unterliegt auch eine statistische Auswertung, die – wie im obigen Beispiel – zu einem anonymen Ergebnis führt, den Vorschriften der DS-GVO.

1 Siehe insbesondere Art. 5 Abs. 2 DS-GVO

2 Art. 35 DS-GVO

3 Art. 36 DS-GVO

Datenschutzprüfungen sind zukünftig nicht mehr nur eine besondere Pflicht bei großen Änderungen, wie beispielsweise bei einer Softwareeinführung. Sie kommen vielmehr bei jeder neuen oder geänderten Verarbeitung personenbezogener Daten zum Tragen, d. h. sie werden eine „alltägliche" Aufgabe. Führungskräfte stehen deshalb vor der Herausforderung, zu erkennen, wann eine Datenschutzprüfung notwendig ist, und diese anzustoßen und fachlich zu begleiten. Das Spannungsfeld zwischen den Datenschutzvorgaben der DS-GVO und den Vorstellungen des Business gilt es dabei zu harmonisieren.

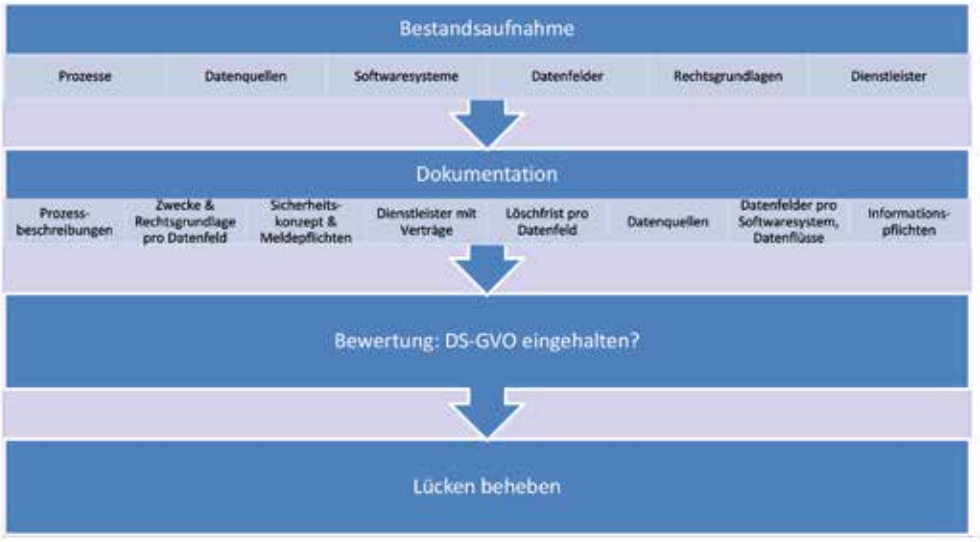

Abbildung 1: Erste Schritte zur Umsetzung der DS-GVO

Auch heute schon ist ein Datenschutzverstoß nicht folgenlos. Beweisverwertungsverbote bei unrechtmäßig erlangten Beweisen, Bußgelder und Schadensersatzansprüche sind hinlänglich bekannt. Die DS-GVO erhöht die „Angriffsfläche" jedoch deutlich durch die Kombination folgender Vorschriften:

- deutlich höhere Transparenzpflichten gegenüber Mitarbeitern und Bewerbern,
- detailliertere Vorgaben, wie personenbezogene Daten verarbeitet werden dürfen,
- expliziter Schadensersatzanspruch – auch bei immateriellen Schäden, zu denen unrechtmäßige Eingriffe in das Persönlichkeitsrecht zählen,
- Beweislastumkehr und
- Bußgelder von bis zu 20 Mio. Euro oder – sofern höher – vier Prozent des weltweiten Jahresumsatzes.

3 Prozessanforderungen

Die Erfahrung zeigt, dass Prozesse gemäß fachlichen Anforderungen und technischen Möglichkeiten gestaltet werden. Dabei wird derzeit höchstens kursorisch geprüft, ob die Verarbeitung personenbezogener Daten grundsätzlich für den mit dem Prozess verfolgten Zweck zulässig ist. Zukünftig muss die datenschutzrechtliche Betrachtung tiefer gehen und die Gestaltung des Prozesses in den Blick nehmen.

Unternehmen müssen durch „geeignete technische und organisatorische Maßnahmen sicherstellen, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden"[4]. Anwendungen wie SAP HCM verarbeiten Daten zu ganz unterschiedlichen Zwecken (beispielsweise Zeiterfassung und Entgeltabrechnung). Bei der Gestaltung der jeweiligen Verarbeitungsschritte muss deshalb darauf geachtet werden, dass nur die erforderlichen Daten verwendet werden.[5] Gleiches gilt auch für die Protokollierung während der Verarbeitung. Die Erforderlichkeit sollte jederzeit belegbar sein. Betrachtet werden muss dabei

- die Menge der erhobenen Daten,
- der Umfang ihrer Verarbeitung,
- die Speicherfrist und
- die Zugänglichkeit.

Für die Speicherung gilt, dass personenbezogene Daten „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist"[6]. Konkret bedeutet das, dass der Personenbezug (Personalnummer, Namen usw.) von den übrigen Daten (Lohngruppe, Alter usw.) trennbar gespeichert werden sollte. Beispielsweise benötigt man für eine Analyse der Altersstruktur im Unternehmen keine Identifizierung der Mitarbeiter.

Auch die Datenqualität wird durch die DS-GVO reguliert. Personenbezogene Daten müssen sachlich richtig und, soweit für den Verarbeitungszweck erforderlich, auf dem neuesten Stand sein.[7] Es sind weiterhin „alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich ge-

4 Art. 25 Abs. 2 DS-GVO

5 Art. 5 Abs. 1 Lit. c) und Art. 25 Abs. 5 DS-GV

6 Art. 5 Abs. 1 Lit. e) DS-GVO

7 Art. 5 Abs. 1 Lit. d) DS-GVO

löscht oder berichtigt werden“[8]. Aus fachlicher Sicht braucht HR richtige und vollständige Daten. Insofern ergeben sich grundsätzlich keine neuen Anforderungen. Die DS-GVO nimmt jedoch das Unternehmen explizit in die Verantwortung, „angemessene Maßnahmen“ zu treffen, um die Richtigkeit sicherzustellen. Der pauschale Verweis, die Richtigkeit läge auch im Interesse der Mitarbeiter, dürfte daher nicht als „angemessene Maßnahme“ verstanden werden. Beispielsweise fallen veraltete Notfalltelefonnummern i. d. R. erst im konkreten Notfall auf. Mögliche Maßnahmen sind jährliche Aktualitätsabfragen oder die vertragliche Verpflichtung der Mitarbeiter, Änderungen zu melden.

Unternehmen müssen sicherstellen, dass Personen, die Zugang zu personenbezogenen Daten haben, diese ausschließlich nach Anweisung des Unternehmens verarbeiten.[9] Dies setzt voraus, dass

- Anweisungen z. B. in Form von Arbeitsanweisungen, Prozessbeschreibungen oder Anwendungsmasken gegeben werden und
- Kontrollen auf Einhaltung existieren.

Welche Maßnahmen angemessen sind, muss in einer risikoorientierten Abwägung ermittelt werden.[10] Zu Beweiszwecken sollte diese dokumentiert werden. Die Abwägung verläuft analog zur Erstellung eines IT-Sicherheitskonzepts, dessen Erstellung ebenfalls durch die DS-GVO inhaltlich vorgeschrieben wird.[11] Ausgangspunkt ist dabei der Stand der Technik. Anschließend werden die Implementierungskosten abgewogen gegen

- die Risiken aus der rechtmäßigen und unrechtmäßigen Verarbeitung,
- Art und Umfang der Verarbeitung,
- Umstände der Verarbeitung und
- Zwecke.[12]

Die Abwägung muss aktuell gehalten werden, d. h. es bedarf eines Prozesses, um diese regelmäßig oder anlassbezogen zu prüfen und zu aktualisieren.

4 Einkauf von Produkten und Dienstleistungen

Die Beschaffung oder der Betrieb eines Softwareprodukts, das beispielsweise auch Daten sammelt, die nicht benötigt werden, wäre nach der DS-GVO unzulässig. Es kommt dabei nicht darauf an, ob die gesammelten Daten auch verwendet werden, da die DS-GVO bereits bei der Erhebung ansetzt. Das Einhalten der Löschpflicht – unter Beachtung ggf. geltender Revisions- und Aufbewahrungsvorschriften – zählt grundsätzlich zu den Pflichteigenschaften von Produkten.

Da sich der Stand der Technik weiterentwickelt und Produkte durch Updates plötzlich nicht benötigte Daten zu erheben beginnen können, empfiehlt es sich, diese Aspekte bei der Beschaffung von Hardware- und Softwareprodukten und auch bei der Nutzung von Cloud Services (z. B. Software als a Service) zu berücksichtigen. Die DS-GVO verbietet nicht den Vertrieb von Produkten oder Services, die sich nicht rechtskonform nutzen lassen. Deshalb kann sich ein Einkäufer nicht per se auf die Rechtskonformität verlassen.

Nicht datenschutzkonform nutzbare Produkte und Services verursachen dreifache Kosten:

8 Art. 5 Abs. 1 Lit. d) DS-GVO

9 Art. 32 Abs. 4 DS-GVO

10 Art. 25 Abs. 1 DS-GVO

11 Art. 32 DS-GVO

12 Ausführlicher in Lepperhoff, Niels (2016): Neue gesetzliche Pflichten für IT-Verantwortliche. In: IT-Sicherheit, April 2016

- Anschaffung plus
- Ersatzbeschaffung inklusive Migrationskosten plus
- mögliches Bußgeld von bis zu 10 Mio. Euro oder – sofern höher – zwei Prozent des Umsatzes des Vorjahres.

Eine umfangreichere Prüfung von Produkten und Leistungen vor der Beschaffung unter Einbeziehung des Datenschutzbeauftragten und des IT-Sicherheitsbeauftragten ist dringend empfohlen. Geprüft werden sollte neben der grundsätzlichen fachlichen und kaufmännischen Eignung u. a. auch, ob

- sich die Erhebung nicht benötigter Daten abschalten lässt,
- alle Daten automatisch nach Regeln gelöscht werden können,
- eine Zugriffssteuerung auf Rechtebasis möglich ist (sofern notwendig),
- die Datenhaltung eine Aufhebung des Personenbezugs zulässt,
- eine Integration in die Sicherheitsarchitektur des Unternehmens keine neuen Risiken oder Lücken schafft und
- die eingebauten Sicherheitsmaßnahmen dem Stand der Technik entsprechen und angemessen sind.

5 Zusammenarbeit mit dem Betriebsrat

Für die Betriebsratsarbeit wird die DS-GVO genauso gelten wie heute das BDSG. Deshalb bietet es sich an, den Betriebsrat möglichst frühzeitig über die Neuerungen zu informieren. Nach der bisherigen Rechtsprechung ist er für die Einhaltung der Datenschutzgesetze selbst verantwortlich.[13] Wenn diese Rechtsprechung fortbesteht – wofür ihre Herleitung aus dem Betriebsverfassungsgesetz spricht –, dann eröffnet sich für den Arbeitgeber noch stärker als heute die Haftung für die Handlungen des Betriebsrats.

Der Arbeitgeber wird auch zukünftig für jede Datenweitergabe an oder Einsichtnahme durch den Betriebsrat eine erlaubende gesetzliche Vorschrift benötigen.

Bestehende Betriebsvereinbarungen können Regeln zum Datenschutz oder auch zur Prozessgestaltung enthalten. Um sicherzustellen, dass die Betriebsvereinbarungen, die über Mai 2018 hinaus gültig sein sollen, datenschutzkonform sind, ist eine Prüfung dringend angeraten. Die Prüfung sollte beispielsweise auch umfassen, ob die Betroffenenrechte im Vergleich mit den Regeln in der DS-GVO eingeschränkt wurden.

6 Fazit

Mit der Datenschutz-Grundverordnung nimmt die Verantwortung von Führungskräften für die Einhaltung von Datenschutzvorschriften zu. Alltägliche Aufgaben, wie z. B. Prozessfestlegungen oder -änderungen sowie die Beschaffung von Produkten und Leistungen, bedürfen umfangreicherer Datenschutzprüfungen als früher.

Die zweijährige Übergangszeit sollte genutzt werden, den eigenen Bereich auf die neuen Anforderungen hin anzupassen.

13 Gola/Wronka (2013), Handbuch Arbeitnehmerdatenschutz – Rechtsfragen und Handlungshilfen, 6. Auflage, Rdnr. 1950 f.

DR. NIELS LEPPERHOFF
Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH