Checkliste DSGVO

Einleitung

Ab dem 25. Mai 2018 finden die Regelungen der europäischen Datenschutz-Grundverordnung Anwendung. Die zweijährige Umsetzungsfrist ist fast abgelaufen, noch weniger als ein Monat bleibt für die letzten Anpassungen. Vor diesem Hintergrund ist jetzt eine gute Gelegenheit, noch einmal den Stand der eigenen Vorbereitungen zu überprüfen. Wir haben hierzu eine Übersicht erstellt, die wesentliche Vorkehrungen zur Umsetzung der neuen rechtlichen Anforderungen beschreibt und zusammenfasst. Bestandteil unserer Übersicht ist auch eine zusammenfassende Checkliste über wichtige Maßnahmen, die von allen Unternehmen bis zum 25. Mai 2018 umgesetzt sein sollten.

Bereits in der Vergangenheit haben wir in den letzten Newslettern über viele Themen ausführlich berichtet; die jeweils einschlägigen Schwerpunktthemen sind dabei entsprechend verlinkt. Bei Bedarf können Sie sich mit Hilfe dieser Unterlagen nochmals vertieft mit einzelnen datenschutzrechtlichen Vorgaben befassen.

Überprüfung der Datenverarbeitungsprozesse

Die Vorgaben für die Verarbeitung personenbezogener Daten werden durch die DSGVO in vielen Teilen verändert. Hierdurch ergibt sich die Notwendigkeit, alle Datenverarbeitungsprozesse mit Hinblick auf die neuen rechtlichen Anforderungen der DSGVO zu überprüfen. Im Rahmen der Überprüfung sollten alle Datenverarbeitungsprozesse insbesondere an den folgenden Grundprinzipien des Datenschutzes gemessen werden:

- Erlaubnisvorbehalt (Zulässigkeit des Umgangs mit personen bezogenen Daten bedarf grundsätzlich der gesetzlichen Erlaubnis)
- Zweckbindungsgrundsatz
- Verarbeitung nach Treu und Glauben
- Transparenz (Informationen, Benachrichtigung und Auskunftserteilung)
- Grundsätze der Datenminimierung, Speicherbegrenzung und Privacy by Design / Default
- Richtigkeit, Integrität und Vertraulichkeit der Daten
- Datensicherheit (Schutz vor Verlust, Sabotage, unbefugtem Zugriff)

Unter Beachtung dieser Grundprinzipien kann sich sowohl ein inhaltlicher Anpassungsbedarf der Prozesse ergeben als auch die Notwendigkeit zur Anpassung der begleitenden Rechtstexte und Erläuterungen. In jedem Fall sollten alle Einwilligungs- oder Datenschutzerklärungen überarbeitet werden.

Soweit im Rahmen der Datenverarbeitung auch eine Datenübermittlung an andere Unternehmen erfolgt, muss dies zukünftig für die betroffene Person transparent sein. Die bisher schon bekannte Privilegierung für Dienstleister, die unter der Verantwortung und nach Weisung des Auftraggebers tätig werden (Auftragsverarbeitung) bleibt aber grundsätzlich bestehen. Dennoch ist es erforderlich, auch die schon bestehenden Vereinbarungen zur Auftragsverarbeitung anzupassen. Insoweit kann es hilfreich sein, alle im Unternehmen eingesetzten Dienstleister in einer Liste zusammenzutragen und diese zum Zweck der Anpassung der bisherigen Vereinbarung einheitlich zu kontaktieren.

Bestellung des Datenschutzbeauftragten

Die Regelungen zur Bestellung eines Datenschutzbeauftragten sind für Unternehmen in Deutschland weitgehend beibehalten worden. Auch weiterhin muss zwingend ein Datenschutzbeauftragter bestellt werden, soweit in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 BDSG-neu). Alle anderen Unternehmen sollten überprüfen, inwieweit gegebenenfalls eine freiwillige Bestellung sinnvoll ist, um sich bei der Umsetzung der neuen Anforderungen professionell unterstützen zu lassen. Neu ist die Pflicht zur Veröffentlichung und Meldung der Kontaktdaten des Datenschutzbeauftragten (Art. 37 Abs. 7 DSGVO).

Erfüllung der Nachweispflicht

Unternehmen unterliegen zukünftig im Rahmen der Datenverarbeitung einer erhöhten Nachweispflicht (Art. 5 Abs. 2 DSGVO). Dies bedeutet, dass sie in der Lage sein müssen, die Einhaltung der datenschutzrechtlichen Anforderungen an die Verarbeitung von personenbezogenen Daten auf geeignete Weise zu belegen. Die Aufsichtsbehörden sind berechtigt, auf dieser Grundlage die Datenverarbeitung im jeweiligen Unternehmen zu prüfen. Ein derartiger Nachweis wird nur durch eine

umfangreiche datenschutzrechtliche Dokumentation erbracht werden können. Insoweit ist jedem Unternehmen zu empfehlen, eine strukturierte Dokumentation der eigenen datenschutzrechtlichen Aktivitäten zu erarbeiten.

Ein zentraler Baustein der Dokumentation sollte zukünftig das Datenschutzkonzept sein, das die wesentlichen Maßnahmen und Ziele des Datenschutzes im Unternehmen zusammenfasst sowie die allgemeinen Anforderungen für das Unternehmen konkretisiert. Bei Bedarf können zusätzlich die einzelnen Aktivitäten in bestimmten Bereichen separat dokumentiert werden. So ist es empfehlenswert, geplante und durchgeführte Maßnahmen zur Vermittlung von datenschutzrechtlichem Wissen im Unternehmen in einem Schulungskonzept zusammenzufassen. Weiterhin sollten alle Mitarbeiter – wie bisher schon gesetzlich vorgeschrieben – auf das Datengeheimnis verpflichtet werden. Für den Umgang bei Datenschutzverstößen sollte ebenfalls ein klares Vorgehen definiert, schriftlich festgehalten und im Unternehmen bekannt gemacht werden, damit die Vorbereitungen nachgewiesen und im Ernstfall die knappen Fristen eingehalten werden können.

Zum Nachweis der Einhaltung der datenschutzrechtlichen Vorschriften und zur Selbstkontrolle ist zudem von jedem Unternehmen ein Verzeichnis der Verarbeitungstätigkeiten zu führen, das den Mindestanforderungen gem. Art. 30 DSGVO zu genügen hat. Zusätzlich sind für Verarbeitungsvorgänge, die ein großes Risiko für die Rechte der Betroffenen zur Folge haben, gesonderte schriftliche Dokumentationen in Form von Datenschutz-Folgeabschätzungen durchzuführen. Es bietet sich dabei häufig an, die Überprüfung der einzelnen Datenverarbeitungsprozesse auf Basis der Beschreibung der jeweiligen Verarbeitungstätigkeit vorzunehmen oder im Rahmen der Überprüfung die Beschreibung zu erstellen.

Der Datenschutzbeauftragte sollte seine Tätigkeiten ebenfalls dokumentieren, beispielsweise im Rahmen von jährlichen Tätigkeitsberichten.

Vorbereitung auf Anfragen von Betroffenen

Unter der DSGVO werden die Rechte der von der Datenverarbeitung betroffenen Personen gestärkt. Zusätzlich zu den aus dem bisherigen Datenschutzrecht bekannten Betroffenenrechten gibt es teilweise auch neue Ansprüche der Betroffenen, die Unternehmen zu erfüllen haben.

Zur Vorbereitung auf die Anwendung der Regelungen der DSGVO ist allen Unternehmen zu empfehlen, bereits im Vorfeld gemeinsam mit den Fachabteilungen zu prüfen, wie die Erfüllung der Betroffenenrechte umgesetzt werden kann und wie der Umgang mit Anfragen der Betroffenen praktisch ablaufen soll. Hierfür ist es vielfach zielführend, wenn typische Konstellationen wie Anfragen auf Löschung und Auskunftsbegehren gemeinsam mit den zuständigen Mitarbeitern vorbereitet und die erforderlichen Abläufe konkret geprüft werden. Dies schafft Sicherheit bei den Mitarbeitern im Umgang mit den Betroffenenrechten und zeigt zugleich, ob den Anfragen der Betroffenen tatsächlich innerhalb der vorgegebenen Fristen entsprochen werden kann.
In diesem Zusammenhang kann auch überprüft werden, inwieweit das neue Recht auf Datenportabilität im Unternehmen umgesetzt werden kann.

Zusammenfassende Checkliste

- ✔ Einhaltung der Grundprinzipien des Datenschutzes bei allen Datenverarbeitungsprozessen
- ✔ Aktualisierung von Rechtstexten mit Bezug zum Datenschutz
- ✔ Abschluss von Vereinbarungen in Fällen der Auftragsverarbeitung
- ✔ Bestellung eines Datenschutzbeauftragten
- ✔ Festlegung eines Datenschutzkonzepts
- ✔ Durchführung von strukturierten Schulungsmaßnahmen
- ✔ Festlegung und Bekanntmachung eines Konzepts zum Vorgehen bei Datenschutzverstößen
- ✔ Führung eines Verzeichnisses der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO
- ✔ Vorbereitung auf Anfragen von Betroffenen

Die Checkliste enthält wesentliche Maßnahmen zur Umsetzung der Anforderungen der DSGVO, ohne allerdings Anspruch auf Vollständigkeit zu erheben.

Robert Bommel, LL.M. / Dr. Sebastian Meyer, LL.M.

Kontakt:

BRANDI Rechtsanwälte Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt
Datenschutzauditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 115
M sebastian.meyer@brandi.net

www.brandi.net