ENDSPURT BEI DER UMSETZUNG DER DS-GVO

Tim Wybitul und Isabelle Brams

(veröffentlicht im BvD Fachmagazin für den Datenschutz Ausgabe 1/2018)

Einleitung

Ab dem 25. Mai 2018 gilt für die Unternehmen in der EU verbindlich die EU-Datenschutzgrundverordnung („DS-GVO“). Zur Umsetzung der komplexen Anforderungen der DS-GVO bleibt den Unternehmen somit nur noch ein knapper Umsetzungszeitraum. In den wenigen verbleibenden Monaten ist eine lückenlose Umsetzung der DS-GVO regelmäßig kaum noch möglich. Was sollten Unternehmen also tun, wenn sie bislang noch keine Umsetzungsschritte unternommen haben? Der vorliegende Überblick gibt Unternehmen eine Art „Notfallplan“ an die Hand, mit dem sie zumindest die wichtigsten Anforderungen der DS-GVO noch in angemessenen Umfang umsetzen können. Dies soll den Unternehmen helfen, drohende Haftungsrisiken zu verringern. Dies gilt nicht nur für mögliche Bußgelder durch die Datenschutzaufsichtsbehörden, sondern auch für Schadensersatzklagen Betroffener. Der Beitrag beschreibt zentrale Anforderungen der DS-GVO. Er zeigt, wie Unternehmen diese mithilfe von „Notfallmaßnahmen“ noch in einem angemessenen Umfang umsetzen können.

Die zentralen Anforderungen der DS-GVO auf einen Blick

Die DS-GVO enthält eine Vielzahl verschiedener Vorgaben für die Unternehmen. Nicht alle dieser Anforderungen werden in der Praxis voraussichtlich von hoher Relevanz sein. Da viele Unternehmen in der Kürze der Zeit nicht mehr sämtliche Vorgaben der DS-GVO umsetzen können, sollten sie sich auf wesentliche Anforderungen konzentrieren. Im Rahmen der hierfür erforderlichen Risikoanalyse sollten Unternehmen insbesondere die Höhe der möglichen Bußgelder im Blick behalten. Dabei sollten Unternehmen auch berücksichtigen, wie wahrscheinlich es ist, dass mögliche Schäden von betroffenen Personen oder Datenschutzaufsichtsbehörden geltend gemacht werden.

Der folgende Abschnitt soll Unternehmen für ihre Risikoanalyse einige Leitlinien an die Hand geben. Die Autoren zeigen die aus ihrer Sicht wesentlichen Anforderungen der DS-GVO, die Unternehmen nicht zuletzt zur Vermeidung von Compliance-Verstößen möglichst zeitnah umsetzen sollten. Dazu zählen insbesondere die in Art. 5 DS-GVO festgelegten Datenschutzgrundsätze.

• Zweckfestlegung:

Bei der erstmaligen Erhebung oder sonstiger Verarbeitung von personenbezogenen Daten müssen Unternehmen die Zwecke festlegen, für die sie die jeweiligen personenbezogenen Daten verarbeiten, Art. 5 Abs. 1 lit. b) DS-GVO. Unternehmen sollten bis zum 25. Mai 2018 grundlegende Prozesse entwickelt haben, um sicherzustellen, dass die Zwecke der Verarbeitung tatsächlich vor der Verarbeitung festgelegt und dokumentiert werden.

• Transparenz:

Die DS-GVO verpflichtet Unternehmen dazu, die Datenverarbeitungen für die Betroffenen möglichst transparent auszugestalten, Art. 5 Abs. 1 lit. a) DS-GVO. Dieser Transparenzgrundsatz wird durch die Art. 12 ff. DSGVO ausgestaltet. Danach müssen Unternehmen die betroffenen Personen über die geplanten Datenverarbeitungsvorgänge umfassend informieren. Unternehmen sollten bis zum 25. Mai 2018 grundlegende Strukturen entwickeln, um den

Informationspflichten unter der DS-GVO nachzukommen. Beispielsweise bietet es sich an, Muster für derartige Informationsschreiben aufzusetzen.

• Rechtmäßigkeitsgrundsatz:

Personenbezogene Daten dürfen nur verarbeitet werden, wenn für die Verarbeitung eine wirksame Rechtsgrundlage besteht, Art. 5 Abs. 1 lit. a) DS-GVO. Unternehmen sollten daher zumindest ihre zentralen Datenverarbeitungsvorgänge dahingehend überprüfen, ob ihnen eine wirksame Rechtsgrundlage zugrunde liegt. Mögliche Ermächtigungsgrundlagen ergeben sich insbesondere aus Art. 6 und Art. 9 Abs. 2 DS-GVO. Speziell im Beschäftigungskontext sind als Rechtsgrundlagen zudem Art. 88 DS-GVO und § 26 des neuen Bundesdatenschutzgesetzes („BDSG-neu“) relevant.

• Grundsatz Datenminimierung:

Unternehmen dürfen grundsätzlich nur in dem Maße personenbezogene Daten erheben und verarbeiten, wie dies für die Erreichung des zuvor festgelegten Zwecks erforderlich ist, Art. 5 Abs. 1 lit. c) DSGVO. Mittel, um diese Vorgaben umzusetzen, sind insbesondere die Anonymisierung und Pseudonymisierung von personenbezogenen Daten. Unternehmen sollten daher zumindest rudimentär überprüfen, welche Verarbeitungen auch mit anonymisierter oder pseudonymisierten Daten möglich sind.

• Löschung von Daten:

Unternehmen müssen sicherstellen, dass personenbezogene Daten ab dem 25. Mai 2018 nach Maßgabe von Art. 17 Abs. 1 DS-GVO gelöscht werden. Im Regelfall sind personenbezogene Daten zu löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind. Gesetzliche Aufbewahrungspflichten können aber im Einzelfall eine längere Speicherung bedingen. Es ist aber vielfach nicht realistisch sein, dass Unternehmen bis zum 25. Mai 2018 umfassende Löschkonzepte entwickeln können. Solche Unternehmen sollten aber zumindest für die wichtigsten Datenverarbeitungsvorgänge konkrete Löschfristen bestimmen und festlegen.

• Datenschutzfolgenabschätzung:

Unternehmen sind gemäß Art. 35 DS-GVO verpflichtet, in den dort festgelegten Fallgruppen eine Datenschutzfolgenabschätzung vorzunehmen. Sie sollten sich daher bis zum 25. Mai 2018 zumindest einen guten Überblick darüber verschaffen, welche Datenverarbeitungsvorgänge zukünftig einer Datenschutzfolgenabschätzung unterliegen könnten.

• Sicherheit der Verarbeitung:

Auf der Basis einer entsprechenden Risikoanalyse müssen Unternehmen ein angemessenes Schutzniveau in Bezug auf die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten. Dabei sollten sie insbesondere Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten in Betracht ziehen.

• Betroffenenrechte und Beschwerdemanagement:

Die DS-GVO räumt den von der Datenverarbeitung betroffenen Personen umfangreiche Rechte ein (sog. „Betroffenenrechte“). Dies beinhaltet unter anderem Rechte auf Auskunft oder Berichtigung, Art. 15 ff. DS-GVO. Unternehmen sollten bis zum 25. Mai 2018 zumindest grundsätzlich in der Lage sein, die Beschwerden und Anfragen Betroffener entgegenzunehmen und ohne Fehler oder Versäumnisse zu beantworten.

• Verhalten bei Datenschutzverstößen:

Gemäß Art. 33 DS-GVO müssen Unternehmen Datenschutzverstöße grundsätzlich innerhalb von 72 Stunden bei der zuständigen Datenschutzaufsichtsbehörde melden. Bringt die Datenpanne zudem voraussichtlich ein hohes Risiko für die Betroffenen mit sich, muss das Unternehmen auch diese informieren, Art. 34 DS-GVO. Um diesen Anforderungen Rechnung zu tragen, sollten Unternehmen bis zum 25. Mai 2018 zumindest rudimentäre Prozesse entwickeln, um die rechtzeitige Benachrichtigung der Aufsichtsbehörden (und gegebenenfalls der betroffenen Personen) im Falle eines Datenschutzverstoßes sicherzustellen.

• Einwilligungen:

Unternehmen sollten bis zum 25. Mai 2018 auch ihre Einwilligungspraxis auf den Prüfstand stellen. Denn vielfach entsprechen bestehende Einwilligungserklärungen nicht den Vorgaben von Art. 7 und 8 DS-GVO. Zwar gehen die deutschen Datenschutzaufsichtsbehörden davon aus, dass bestehende Einwilligungserklärungen grundsätzlich auch unter der DS-GVO weiter wirksam bleiben können. Ob Gerichte diese Rechtsauffassung künftig teilen, ist aber zweifelhaft. Die DS-GVO jedenfalls bietet für diese großzügige Ansicht keine klaren Anhaltspunkte. Bei der Einholung neuer Einwilligungen sind jedoch zukünftig zwingend die Vorgaben der DS-GVO zu beachten. Unternehmen sollten daher bis zum 25. Mai 2018 neue Muster für Einwilligungen erstellen, die den Vorgaben der Art. 7 und 8 DS-GVO entsprechen

• Anpassung von Verträgen:

Unternehmen müssen grundsätzlich ihre Verträge, die Datenverarbeitungen zum Gegenstand haben, auf ihre Vereinbarkeit mit der DS-GVO überprüfen. Dies gilt insbesondere auch für bestehende Auftragsverarbeitungsverträge. Solche Verträge müssen zukünftig den Anforderungen von Art. 28 Abs. 3 DS-GVO genügen. Doch auch für Arbeitsverträge und Verträge mit Kunden kann sich Anpassungsbedarf ergeben. Auch in diesem Zusammenhang sollten Unternehmen Notfallstrategien entwickeln, um gegebenenfalls wichtige Verträge auf ihre Vereinbarkeit mit der DS-GVO zu überprüfen.

• Anpassung von Betriebsvereinbarungen:

Unternehmen müssen auch ihre bestehenden Betriebsvereinbarungen auf den Prüfstand stellen, sofern diese Datenverarbeitungen zum Gegenstand haben. Bei dieser Prüfung werden insbesondere die Vorgaben von Art. 88 DS-GVO und § 26 BDSG relevant. So müssen Betriebsvereinbarungen zukünftig insbesondere angemessene Maßnahmen enthalten, um die berechtigten Interessen und Persönlichkeitsrechte der betroffenen Mitarbeiter zu wahren. Zudem müssen auch Betriebsvereinbarungen künftig grundsätzlich den Anforderung von Art. 5 DS-GVO genügen, § 26 Abs. 5 BDSG (vgl. zu diesem Thema auch einen Beitrag auf unserem Blog http://hoganlovells-blog.de/2018/01/12/DS-GVO-und-betriebs vereinbarungen-in-der-praxis-handlungsemp-fehlun gen-und-checkliste/)

„Notfallmaßnahmen“ zur Umsetzung der DS-GVO

Für viele Unternehmen wird es kaum realistisch sein, bis zum 25. Mai 2018 sämtliche der im ersten Teil genannten besonders wesentlichen Anforderungen vollumfänglich umzusetzen. Denn die Umsetzung der DS-GVO erfordert regelmäßig ein effektives Zusammenwirken vieler verschiedener Stellen und Abteilungen im Unternehmen. Dies in der Kürze der Zeit zu koordinieren, dürfte viele Unternehmen vor nicht überwindbare Herausforderungen stellen.

Der folgende Abschnitt stellt mögliche Notfallmaßnahmen dar, um zumindest die größten Haftungsrisiken zu verringern. Unternehmen sind daher gut beraten, die im Folgenden dargestellten Maßnahmen bis zum 25. Mai 2018

anzugehen oder zumindest in die Wege zu leiten.

Überprüfung zentraler Datenverarbeitungsvorgänge

Allein aus praktischen Gründen ist es für viele Unternehmen kaum machbar sämtliche Datenverarbeitungsvorgänge auf ihre Vereinbarkeit mit der DS-GVO zu überprüfen. Unternehmen sollten bis zum 25. Mai 2018 aber zumindest ihre zentralen und wichtigsten Datenverarbeitungsvorgänge auf den Prüfstand stellen. Dabei sollten Unternehmen insbesondere die Vorgaben von Art. 5 DS-GVO beachten und umsetzen. Soweit möglich, sollten Unternehmen eine Anonymisierung oder Pseudonymisierung von Datensätzen prüfen.

Einführung eines Dokumentationssystems

Die DS-GVO legt den Unternehmen umfassende Dokumentationspflichten auf. So müssen Unternehmen nach Art. 5 Abs. 2, 24 Abs. 1 DS-GVO nachweisen können, dass sie personenbezogene Daten nach Maßgabe der Verordnung verarbeiten. Dieser Vorgabe kommt insbesondere bei möglichen Schadensersatzklagen betroffener Personen eine große Bedeutung zu. Denn Art. 24 Abs. 1 DS-GVO beinhaltet eine Beweislastumkehr. Unternehmen müssen somit nicht nur nachweisen können, dass sie die allgemeinen Anforderungen der DS-GVO ordnungsgemäß umgesetzt haben. Zudem obliegt ihnen auch die Beweislast, dass die im jeweiligen Rechtsstreit maßgeblichen Datenverarbeitungen im Einklang mit der DS-GVO erfolgt sind. Die DS-GVO trifft keine Aussage dazu, wie das Dokumentationssystem ausgestaltet sein muss. Um eine effektive Umsetzung der Dokumentationspflichten sicherzustellen, wird vielfach aber die Einführung eines Datenschutzmanagement-Systems erforderlich sein. Ein wichtiger Bestandteil des Dokumentationssystems ist dabei das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO. Dieses Verzeichnis enthält spezifische Beschreibungen der einzelnen Verarbeitungsvorgänge. Daneben sollten Unternehmen auch weitere Strategien entwickeln, um sämtliche Verarbeitungsvorgänge umfassend zu dokumentieren. Unternehmen sollten ein Dokumentationssystem entwickeln, das ihnen in späteren Schadensersatzprozessen oder Bußgeldverfahren eine Dokumentation an die Hand gibt, mit deren Hilfe sie die Einhaltung der Anforderung der DS-GVO nachweisen können. Ziel sollte es sein, gleichsam „auf Knopfdruck“ die relevante Dokumentation für den konkret Betroffenen generieren und vorlegen zu können.

Einbindung des Datenschutzbeauftragten

Unternehmen sind gut beraten, ihren Datenschutzbeauftragten bei der „Notfallplanung“ eng einzubeziehen. Der Datenschutzbeauftragte kann regelmäßig hilfreiche Hinweise und Anregungen geben, um die Anforderungen der DS-GVO möglichst zeitnah und in angemessenen Umfang umzusetzen.

Anpassung der wichtigsten Vertragsdokumente

In der Kürze der Zeit wird ein Großteil der Unternehmen seine bestehenden Verträge und Vertragsmuster wohl kaum vollumfänglich auf die Vereinbarkeit mit der DS-GVO überprüfen können. Solche Unternehmen sollten aber zumindest ihre wichtigsten und zentralen Verträge überprüfen und gegebenenfalls anpassen. Dies gilt insbesondere für Auftragsverarbeitungsverträge. Unternehmen sollten daher möglichst zeitnah auf ihre Auftragsverarbeiter zugehen und über eine Anpassung der bestehenden Verträge verhandeln. Dies hilft nicht nur dem Unternehmen, Haftungsrisiken zu entgehen. Auch den Auftragsverarbeitern wird vielfach an einer zeitnahen Umsetzung der DS-GVO gelegen sein. Denn unter der DS-GVO sind auch sie deutlich höheren Haftungsrisiken ausgesetzt als nach geltendem Recht.

Abschluss einer Rahmenbetriebsvereinbarung DS-GVO

Viele Unternehmen verfügen über eine Vielzahl von Betriebsvereinbarung. Es ist daher nicht realistisch, dass die Unternehmen sämtliche Betriebsvereinbarungen, die Datenverarbeitungen zum Gegenstand haben, auf ihre Vereinbarkeit mit der DS-GVO überprüfen und gegebenenfalls anpassen. Um die Anpassung zu erleichtern, hat es sich in der Praxis als sinnvoll erwiesen, eine Rahmenbetriebsvereinbarung DS-GVO abzuschließen. Eine solche Rahmenbetriebsvereinbarung kann die Anforderungen, die die DS-GVO an Betriebsvereinbarungen stellt, beschreiben und für bestehende Betriebsvereinbarungen umsetzen. Unternehmen sind daher gut beraten, zeitnah auf ihre Betriebsräte zuzugehen und in Verhandlungen zum Abschluss einer solchen Rahmenbetriebsvereinbarung einzutreten.

Fazit

Die DS-GVO legt Unternehmen zahlreiche komplexe Anforderungen auf, deren Umsetzung die Unternehmen – nicht zuletzt wegen des knappen Umsetzungszeitraums – vor erhebliche Herausforderungen stellen. Unternehmen, die die DS-GVO bislang noch nicht umgesetzt haben, sind daher gut beraten, möglichst schnell letzte Maßnahmen zu ergreifen, um zumindest die größten Haftungsrisiken zu vermeiden. Die Unternehmen sollten daher möglichst zeitnah einen Notfallplan entwickeln, um die Einleitung von kurzfristigen Maßnahmen zur Umsetzung der DS-GVO sicherzustellen. Zudem sollten Unternehmen sich darauf einstellen, dass neben Bußgeldverfahren auch mögliche Schadensersatzklagen drohen. Manche Unternehmen mit hohem Risikopotenzial schreiben derzeit schon erste Textbausteine für Schriftsätze zu ihrer effektiven Verteidigung vor Gericht vor.