EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) :

VERSCHÄRFTE HAFTUNGSRISIKEN FÜR GESCHÄFTSFÜHRER AB MAI 2018 UND IHRE VERMEIDUNG – EIN ÜBERBLICK

Susanne Schröder, Rechtsanwältin, Fachanwältin für Arbeitsrecht, Partnerin, und
Dr. Berit Kochanowski LL.M., Rechtsanwältin,
BTU SIMON GmbH Rechtsanwaltsgesellschaft, Steuerberatungsgesellschaft

Ab 25.05.2018 gilt die Datenschutzgrundverordnung (DSGVO – VO EU 2016/679) und zugleich tritt ein darauf beruhendes neues Bundesdatenschutzgesetz (BDSG) in Kraft. Die DSGVO wird damit unmittelbar geltendes Recht, ohne dass es hierzu einer gesonderten Umsetzung ins nationale Recht bedarf. Ziel dieser VO ist es dem Datenschutz insbesondere in der Praxis der Unternehmen mehr Geltung zu verschaffen. Damit verbunden sind präzisierte Datenschutzregelungen mit entsprechenden Anforderungen an die Compliance. Die für den Fall von Verletzungen der Datenschutzbestimmungen in der DSGVO vorgesehenen Bußgelder sind hoch. Dies sollte jedoch nicht der einzige Grund sein, sich als Geschäftsführer mit dem Datenschutz auseinander zu setzen, denn der mit einer „Datenpanne" verbundene Reputationsverlust ist immens und kann dem Unternehmen erheblichen Schaden zufügen.

1. Persönliche Verantwortung des Geschäftsführers

Der Geschäftsführer hat nach § 43 GmbHG die Geschäfte der Gesellschaft mit der Sorgfalt eines ordentlichen Geschäftsmanns zu führen und von dieser Schäden abzuwenden. Er hat daher dafür zu sorgen, dass die Gesellschaft alle sie treffenden rechtlichen Verpflichtungen einhält und dementsprechend keine Bußgelder oder gar Schadensersatzforderungen anfallen. Die Rechtsprechung anerkennt mittlerweile durchwegs eine Verpflichtung der Geschäftsführung, ein Compliancesystem zu etablieren, um Rechtsverstößen durch die Gesellschaft oder deren Mitarbeiter vorzubeugen[1]. Dies bedeutet, dass ein Geschäftsführer „im Außenverhältnis sämtliche Vorschriften einhalten [muss], die das Unternehmen als Rechtssubjekt treffen" und dafür verantwortlich ist, „dass das Unternehmen so organisiert wird, dass keine Gesetzesverletzungen stattfinden und eine auf Schadensprävention und Risikokontrolle angelegte Compliance-Organisation" eingerichtet wird[2]. Ein unzureichendes Compliance-System und/oder dessen unvollständige bzw. fehlende Überwachung stellen eine Pflichtverletzung dar. Datenschutz ist eine gesetzliche Pflicht, die das Unternehmen einhalten muss, um „compliant" zu sein. Wird das Thema Datenschutz vernachlässigt und die notwendigen Vorgaben nicht eingehalten, kann sich ein Geschäftsführer insbesondere auch gegenüber der Gesellschaft schadensersatzpflichtig machen. Damit treffen die Geschäftsführer selbst die Verantwortung und gegebenenfalls auch die Haftung für die Einhaltung der Vorgaben der DSGVO. Die Anforderungen, die sich daraus ergeben, werden oft als bloßes Problem der IT-Compliance verkannt. Die DSGVO verpflichtet aber die Unternehmen dazu, in jedem Einzelfall und für jeden Unternehmensbereich zu hinterfragen, ob, in welchem Umfang und in welcher Form persönliche Daten erhoben und verarbeitet werden sollen oder müssen.

2. Anwendungsbereich

Die DSGVO richtet sich an alle Unternehmen der Privatwirtschaft und deren Niederlassungen in der EU, die personenbezogene Daten verarbeiten. Diese sind „Verantwortliche" nach Art. 4 Z 7 der DSGVO. Sie gilt jedoch

1) LG München I, 10.12.2013, 5 HKO 1387/10, Für Vorstände einer AG siehe DCGK 2017 4.1.3 Compliancemanagementsystem und 4.1.4 Risikomanagementsystem
2) s.FN 1

auch für Verantwortliche in Drittstaaten, sofern sich deren Angebot an Waren oder Dienstleistungen an Personen innerhalb der EU richtet („Marktortprinzip“[3]).

Entscheidet nicht nur eine Stelle alleinverantwortlich über die Daten, so sieht die DSGVO eine gemeinsame Verantwortlichkeit vor (Art. 26 DSGVO), die auf Grundlage einer Vereinbarung nachvollziehbar auch gegenüber den Datenschutzbehörden festgelegt werden muss. Im Zweifel ist das herrschende Unternehmen im Sinne von Art. 4 Nr. 19 DSGVO Verantwortlicher[4].

Personenbezogene Daten sind nach Art. 4 Z 1 der DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Personenbezogene Daten sind also auch die Sozialversicherungsnummer, die IP-Adresse[5], Informationen zu den benutzten Geräten, die E-Mail-Adresse oder auch die Personalakten an sich, aber auch die Informationen zu Geschäftskontakten in anderen Unternehmen.

1. Allgemeine Grundsätze nach Art. 5 der DSGVO

Eine rechtmäßige Datenverarbeitung ist nur in dem Umfang zulässig, als die den vernünftigen Erwartungen der betroffenen Person entspricht und nachvollziehbar ist **(Rechtmäßigkeit, Datenverarbeitung nach Treu und Glauben, Transparenz)**. Daten sind zudem vor unbefugter oder unrechtmäßiger Verarbeitung und vor Verlust, Zerstörung und Schädigung zu schützen **(Integrität und Vertraulichkeit)**.

Daten dürfen nur in dem Umfang verarbeitet werden, als dies dem Zweck ihrer Erhebung angemessen ist **(Zweckbindung)**. Die Verarbeitung ist zudem auf das für die Zwecke der Verarbeitung notwendige Maß zu beschränken **(Datenminimierung)**. Der Grundsatz der Speicherbegrenzung hat zur Folge, dass Daten nur so lange gespeichert werden dürfen, wie es für die Zwecke, für die sie erhoben werden erforderlich ist (Art. 5 Abs 1 lit e DSGV). Ausnahmen bestehen für die Speicherung von Daten zu Archivzwecken im öffentlichen Interesse bzw. für die wissenschaftliche oder historische Forschung sowie für statistische Zwecke.

Mit diesen Einschränkungen geht eine Verpflichtung einher, nicht mehr benötigte Daten so rasch als möglich zu pseudonymisieren, zu anonymisieren und ggf. diese auch zu löschen und Daten ggf. auch zu berichtigen (**Richtigkeit** der Daten).

2. Rechenschaftspflicht des Verantwortlichen

Art. 5 Abs. 2 verpflichtet die Verantwortlichen zur Einhaltung dieser allgemeinen Grundsätze, mehr noch, sie müssen die Einhaltung dieser Verpflichtungen auch nachweisen können. Die Verpflichtungen des Verantwortlichen haben sich damit gegenüber der bisherigen Rechtslage erheblich verschärft.

3. Datenverarbeitung: Verbot mit Erlaubnisvorbehalt

Nach der DSGVO ist die Verarbeitung von Daten nur dann erlaubt, wenn entweder eine wirksame Zustimmung der betroffenen Person oder aber ein legitimes Interesse für die Verarbeitung besteht. Für jeden einzelnen Fall der Datenverarbeitung ist daher zu prüfen und zu dokumentieren, welcher der Erlaubnistatbestände Grundlage für die Verarbeitung ist.

Die Anforderungen an eine **Einwilligung zur Datenverarbeitung** werden neu geregelt. Eine wirksame Einwilligung kann darüber hinaus vom Betroffenen jederzeit widerrufen werden. Deshalb sollten personenbezogene Daten möglichst nur im Ausnahmefall ausschließlich auf Grundlage einer Einwilligung verarbeitet werden. Zugleich muss geprüft werden, ob bereits vorhandene Einwilligungserklärungen noch den Anforderungen der DSGVO entsprechen.

Als **legitimes Interesse an der Verarbeitung** der Daten anerkennt die DSGVO die in Art. 6 Abs 1 lit b - f genannten Umstände, sofern schutzwürdige Interessen des Betroffenen dem nicht entgegenstehen **(Pflicht zur Interessenabwägung)**. Dazu zählen z.B. die Verarbeitung von Daten, die für die Erfüllung eines Vertrages mit dem Betroffenen erforderlich ist. So dürfen die Kundendaten durch ein Reisebüro verarbeitet werden, soweit und in dem Umfang, als dies für den Reisevertrag erforderlich ist. Erlaubt ist die Verarbeitung von Daten auch, wenn der Verantwortliche hierzu rechtlich verpflichtet ist, wie dies beispielsweise bei Daten von Kunden einer Bank („know your customer“) der Fall ist. Die Daten dürfen jedoch nur so lange zur Verfügung gehalten werden,

3) Erwägungsgrund 23
4) Kazemi, DSGVO in der anwaltlichen Beratungspraxis, §2 RN 4
5) EuGH 19.10.2016 RS C – 582/14 Breyer

als das legitime Interesse an der Verarbeitung unter Berücksichtigung der Grundsätze des Art. 5 noch besteht.

Der Zugang zu den Daten ist zu begrenzen. Daten dürfen nur in dem Umfang für Dritte – auch die eigenen Arbeitnehmer – zugänglich sein, als dies für den jeweiligen Zweck der Datenverarbeitung erforderlich ist. Deshalb sind die Daten von Kunden, Geschäftspartnern und Arbeitnehmern spätestens nach Ablauf der einschlägigen Aufbewahrungsfristen zu löschen. Dies ergibt sich auch aus dem ausdrücklich in Art. 17 der DSGVO vorgesehenen **„Recht auf Vergessenwerden"**. Auch hier ist auf entsprechende organisatorische Maßnahmen zu achten („Löschroutinen").

Ergänzend hat der Betroffene ein umfassendes Recht, über die über ihn verarbeiteten Daten und deren Herkunft bereits bei deren Erfassung informiert zu werden bzw. Auskunft darüber zu erhalten und deren Berichtigung zu verlangen (Art. 15, 16 DSGVO). Daneben kann der Betroffene auch die Herausgabe der Daten in einem geeigneten Format verlangen **(„Portabilität der Daten")**.

4. Pflichten des Verantwortlichen

5.1 Datenschutz durch technische und organisatorische Maßnahmen

Es ist seitens der Unternehmensleitung durch organisatorische Maßnahmen sicherzustellen, dass die Regelungen der DSGVO eingehalten werden. Dazu zählen z.B. die Einführung interner Regelungen für die Erstellung des Verzeichnisses der Verarbeitungstätigkeiten, oder die Bestellung des Datenschutzbeauftragten ebenso wie ein System zum Umgang mit Datenpannen oder Mitarbeiterschulungen, sowie die Einführung von Formularen wie etwa eine Datenschutzerklärung. Ergänzend sind technische Maßnahmen zum Datenschutz vorzusehen, entweder durch die Gestaltung der Art der Datenerfassung („privacy by design") z.B. über verstärkte Nutzung von pseudonymisierten und anonymisierten Daten als auch durch Voreinstellungen, die dem Datenschutz dienen („privacy by default") und z.B. die Datenmengen oder den Umfang ihrer Verarbeitung begrenzen oder auch den Zugriff auf die Daten auf einen bestimmten, eingeschränkten Personenkreis beschränken[6].

Ein Datenschutzbeauftragter ist nach § 38 BDSG (neu) jedenfalls zu bestellen, wenn personenbezogene Daten automatisiert verarbeitet werden, sofern mindestens 10 Personen regelmäßig mit der automatisierten Verarbeitung beschäftigt sind.

5.5 Datenübermittlung an Dritte

Innerhalb der EU und innerhalb des Konzerns ist die Datenübermittlung erlaubnisfrei zulässig, sofern die sonstigen Voraussetzungen für eine rechtmäßige Verarbeitung vorliegen, insbesondere die wirksame Zustimmung des Betroffenen.

In Drittstaaten dürfen Daten nur ausnahmsweise übermittelt werden (§ 4b BDSG – Voraussetzung angemessenes Datenschutzniveau beim Empfänger, nicht im Empfängerstaat); Es muss jedenfalls sichergestellt sein, dass das durch die DSGVO unionsweit gewährte Schutzniveau nicht durch die Übermittlung von Daten in Drittstaaten untergraben wird[7]. Im Fall einer Datenübermittlung in ein Drittland ist der Betroffene darüber hinaus über etwaige Garantien, etwa Binding Corporate Rules oder der Vereinbarung von Standardvertragsklauseln, die den Datenschutzstandard der EU sichern sollen, zu unterrichten (Art. 15 i.V.m Art. 46 DSGVO).

Einer Auftragsdatenverarbeitung muss nach Art. 28 Abs. 3 DSGVO stets ein Vertrag zu Grunde gelegt sein, der dem dort vorgesehenen Mindestinhalt entspricht und auch in Textform abgeschlossen werden kann. Deshalb sind Beziehungen zu Auftragsdatenverarbeitern darauf zu überprüfen, ob eine Anpassung der bestehenden Verträge an die DSGVO erforderlich ist.

6. Folgen von Datenschutzverletzungen

6.1 Bußgelder

Die DSGVO enthält gegenüber der bisherigen Rechtslage erheblich verschärfte Bußgeldregelungen, die nach Art. 82 DSGVO ausdrücklich wirksam, verhältnismäßig und abschreckend sein[8] sollen.

Nach Art. 83 Abs. 5 DSGVO können Bußgelder bis zu 20 Mio. EURO oder 4 % des weltweiten Vorjahresumsatzes, je nach dem was höher ist, verhängt werden. Derartige Bußgelder sind vorgesehen, wenn gegen die Grundsätze des Art. 5 der DSGVO verstoßen wird, etwa wenn die

6) Art. 32 DSGVO
7) Erwägungsgrund 101
8) Erwägungsgrund 152

Datenverarbeitung unrechtmäßig war oder es an der erforderlichen (wirksamen) Zustimmung des Betroffenen fehlt. Dieser Bußgeldrahmen ist aber auch bei unzulässiger Datenübermittlung in Drittstaaten anzuwenden.

6. 2 Schadensersatzansprüche des Betroffenen

Werden die Vorgaben der DSGVO verletzt, kann der Betroffene nicht nur eine Beschwerde bei der zuständigen Aufsichtsbehörde einlegen (Art. 77 DSGVO). Ergänzend hat der Betroffene schon nach Art. 82 DSGVO Anspruch auf Schadenersatz gegen den Verantwortlichen oder einen Auftragsverarbeiter[9]. Es besteht nach Art. 82 Abs. 4 eine gesamtschuldnerische Haftung aller an der Datenverarbeitung beteiligten Verantwortlichen. Dieser Schadenersatzanspruch umfasst sowohl materielle und anders als bisher auch immaterielle Schäden. Von dieser Haftung kann sich der Verantwortliche nur befreien, wenn er nachweist (!), dass er in keiner Weise für den Schaden verantwortlich ist. Damit ist faktisch eine Beweislastumkehr festgelegt (Art. 82 Abs. 3 DSGVO, Art. 5 DSGVO).

6.3 Meldepflicht bei „Datenpannen“

Jede Verletzung des Schutzes von persönlichen Daten i.S.v Art. 4 DSGVO löst nach Art. 33 DSGVO eine Meldepflicht des Verantwortlichen aus. Eine Meldung an die Aufsichtsbehörde kann dann unterbleiben, wenn die Verletzung des Datenschutzes voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Ist mit der Verletzung des Datenschutzes voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen verbunden, so ist auch der Betroffene nach Art. 34 unverzüglich von der Verletzung zu verständigen.

Ein Verstoß gegen diese Meldepflichten ist nach Art. 83 Abs. 4 der DSBGO zu ahnden, also mit Geldbußen bis zu 10 Mio. EURO bzw. 2 % des weltweiten Vorjahresumsatzes.

Fazit:

Wenn Sie schon bisher Datenschutz in Ihrem Fokus hatten, dürfte sich der Anpassungsbedarf in erster Linie aus den umfangreichen Dokumentationspflichten ergeben.

Andernfalls sollte jede Analyse mit einer umfassenden Auflistung der vom Unternehmen gespeicherten und eingesetzten personalisierten Daten beginnen. Jedenfalls sind alle Datenverarbeitungen darauf hin zu überprüfen, ob sie mit den Grundsätzen der DSGVO in Einklang stehen.

Die DSGVO enthält keinen Maßnahmenkatalog, den die Verantwortlichen erfüllen müssen, um die Rechenschaftspflichten zu erfüllen. In jedem Fall haben die Unternehmen eine allumfassende Dokumentationspflicht. Der Geschäftsführer sollte daher veranlassen, dass jeder Umgang mit Daten im Unternehmen insbesondere im Fokus der nachstehenden Fragen analysiert, evaluiert und – nicht allein aus Nachweisgründen – dokumentiert wird.

Checkliste:

1. **Was ist die rechtliche Grundlage für die Verarbeitung der Daten?**
2. **Gibt es Interessen des Betroffenen, die einer Verarbeitung entgegenstehen?**
3. **Zu welchem Zweck erfolgt die konkrete Datenverarbeitung?**
4. **Welche Informationsleitlinien wurden eingerichtet und wie wird deren Einhaltung sichergestellt?**
5. **Ist eine Datenschutzfolgenabschätzung vorgesehen?**
5. **Gibt es ein Sperr- oder Löschkonzept?**
6. **Werden Daten ggf. verschlüsselt, pseudonymisiert oder anonymisiert?**
7. **Gibt es ein Prüfkonzept, das die Aktualität der Daten sicher stellt?**
8. **Wie werden Speicherfristen festgelegt und regelmäßig überprüft?**
9. **Gibt es ein Sicherheitskonzept?**
10. **Wie werden die Auskunftspflichten und Meldepflichten bei etwaigen Datenpannen erfüllt (z.B. Einrichtung einer Anlaufstelle, Mitarbeiterschulungen)?**
11. **Sind alle Datenverarbeitungsvorgänge in einem Verarbeitungsverzeichnis korrekt erfasst?**
12. **Sind die bisher verwendeten vertraglichen Grundlagen (z.B. Einwilligungserklärungen, AGB) noch aktuell und DSVGO-konform?**

9) Erwägungsgrund 146