



Neuerungen durch die Europäische Datenschutz-Grundverordnung

Am 14. April 2016 hat das Europäische Parlament das neue Europäische Datenschutzrecht (sog. Datenschutz-Grundverordnung – DS-GVO) verabschiedet. Zwar hat Deutschland bereits jetzt ein hohes Datenschutzniveau, sodass viele der sich nun durch die DS-GVO in der Europäischen Union ergebenden Rechte und Pflichten die nationalen Regelungen lediglich präzisieren und ausgestalten. Teilweise enthält die DS-GVO allerdings auch Neuerungen im Vergleich zum nationalen Recht.

Die Zeit bis zum Inkrafttreten der DS-GVO im Mai 2018 sollten Sie daher nutzen, um die eigenen Datenschutzsysteme an die Vorgaben der DS-GVO anzupassen.

Herausgeber:

IHK Schleswig-Holstein
Arbeitsgemeinschaft der
Industrie- und Handelskammern zu Flensburg, zu Kiel und zu Lübeck
Bergstraße 2, Haus der Wirtschaft, 24103 Kiel
Telefon: (0431) 5194-0
Telefax: (0431) 5194-234
ihk@kiel.ihk.de
www.ihk-schleswig-holstein.de

Ansprechpartner:

Tina Möller
Telefon: (0431) 5194-258
Telefax: (0431) 5194-558
tmoeller@kiel.ihk.de

Ariane Kühnel
Telefon: (0451) 6006-231
Telefax: (0451) 6006-4231
kuehnel@luebeck.ihk.de

Service-Center IHK Flensburg
Telefon: (0461) 806-806
Telefax: (0461) 806-9806
service@flensburg.ihk.de

Stand: August 2016



Rechtscharakter der DS-GVO	3
Die Neuerungen der DS-GVO im Einzelnen	3
1. Erweiterte Transparenz- und Informationspflichten	3
2. Datensicherheit	4
3. "Privacy by Design" und "Privacy by Default"	4
4. Recht auf Vergessenwerden und Recht auf Datenübertragbarkeit	4
5. Einwilligung in die Datenverarbeitung und Einschränkungen im Hinblick auf das Geschäftsmodell "Dienstleistung gegen Daten"	4
6. Datenaustausch im Konzern	5
7. Der Datenschutzbeauftragte	5
8. Neuerungen betreffend die Datenschutzbehörden - One-Stop-Shop-Prinzip	5
9. Erweiterte Bußgeldtatbestände und höherer Bußgeldrahmen	6

Rechtscharakter der DS-GVO

Die DS-GVO ist Verordnung im Sinne des Art. 288 Abs. 2 AEUV, sie gilt in jedem Mitgliedsstaat unmittelbar und direkt. Zugleich geht sie als europäisches Recht den Normen der einzelnen Mitgliedsstaaten vor. Damit verdrängt die Verordnung – soweit sie keine Öffnungsklausel für einzelstaatliche Regelungen enthält – die Vorschriften der Mitgliedsstaaten. Die DS-GVO ist damit ein Meilenstein auf dem Weg zu einheitlichen EU-weiten Regeln für das digitalisierte und globalisierte Marktumfeld. Zudem wird durch die DS-GVO nunmehr ein einheitliches Datenschutzniveau in der EU auch für die Unternehmen, die ihren Sitz außerhalb der EU haben, aber Daten von EU-Bürgern für Dienstleistungen in der EU verarbeiten, etabliert (Markortprinzip).

Die Neuerungen der DS-GVO im Einzelnen:

1. Erweiterte Transparenz- und Informationspflichten

Unternehmen müssen künftig beweisen können, dass sie die Anforderungen der DS-GVO umsetzen. Auch in Gerichtsverfahren müssen Unternehmen insbesondere beweisen können, dass die von ihm vorgebrachten Beweise für Ansprüche gegen Kunden datenschutzkonform erhoben worden sind. Bei Verstößen drohen ggf. Beweisverwertungsverbote, so dass der eigentlich bestehende Anspruch vom Gericht abgewiesen werden könnte.

Unternehmen müssen Personen von der Verarbeitung ihrer personenbezogenen Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache unterrichten. Gegen die Unternehmen besteht ein entsprechender Auskunftsanspruch, ihnen ist auf Anforderung eine Kopie der verarbeiteten personenbezogenen Daten zur Verfügung zu stellen.

Um diese Anforderungen überhaupt erfüllen zu können, sollten Sie ihre IT-Struktur frühzeitig entsprechend einrichten.

Zugleich sind IT-Prozesse zu schaffen, mit denen Sie den neuen, erweiterten Informationspflichten nachkommen können, die weit über die bisherigen Vorgaben der §§ 4 Abs. 3 und 33 BDSG hinausgehen. Denn nunmehr ist Personen, von denen personenbezogene Daten erhoben werden, u.a. folgendes mitzuteilen: Kontaktdaten des Unternehmens (und seines Datenschutzbeauftragten), Zweck der Datenverarbeitung, Speicherdauer, Bestehen von Auskunftsrechten und Rechten auf Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit und Beschwerderechte gegenüber Aufsichtsbehörden.

Bitte beachten Sie, dass die vorgenannten Rechte den Personen nicht schrankenlos gewährt werden, sondern stets unter dem Vorbehalt stehen, dass das jeweilige Unternehmen kein vorrangiges Interesse an der Verarbeitung dieser Daten geltend machen kann. Selbstverständlich können Sie daher etwa die Daten, die Sie zur (Zahlungs-)Abwicklung von Verträgen zwingend benötigen weiterhin verarbeiten, auch wenn Ihnen gegenüber ein (dann unberechtigter) Löschungsanspruch geltend gemacht wird.

Im Übrigen entfallen diese Informationspflichten dann, wenn und soweit der Betroffene bereits über die Information verfügt.

2. Datensicherheit

Nach Art. 32 DS-GVO hat der Unternehmer geeignete Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Diesbezüglich können Sie sich an den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik orientieren, die unter www.bsi.bund.de abrufbar sind.

3. „Privacy by Design“ und „Privacy by Default“

Die IT-Systeme sind nach Art. 25 Abs. 1 und Abs. 2 DS-GVO an den Grundsätzen „Privacy by Design“ und „Privacy by Default“ auszurichten. Hiernach sind IT-Systeme so zu gestalten, dass sie grundsätzlich nur solche personenbezogenen Daten erheben, die zur Erfüllung des jeweiligen Zwecks erforderlich sind. Es gilt das Gebot der Datenminimierung und Pseudonymisierung.

4. Recht auf Vergessenwerden und Recht auf Datenübertragbarkeit

Im Vergleich zu den bisherigen Regelungen des BDSG billigt die DS-GVO betroffenen Personen umfassende Ansprüche auf Löschung ihrer personenbezogenen Daten zu, soweit nicht das Unternehmen vorrangige Gründe für die weitere Verarbeitung der Daten geltend machen kann. Wurden Daten öffentlich gemacht, so sind auch andere Stellen, die diese Daten verarbeiten, von dem Widerspruch des Betroffenen zu informieren.

So sind etwa personenbezogene Daten ohne unangemessene Verzögerung zu löschen, wenn durch die betroffene Person Widerspruch gegen die Verarbeitung dieser Daten eingelegt. Dieser Anspruch würde jedoch etwa dann nicht bestehen, wenn das Unternehmen diese Daten für vorrangige Zwecke weiterhin benötigt, etwa zur Zahlungsabwicklung.

In Ihrem eigenen Interesse sollten Sie die Zeit nutzen, Ihre IT-Systeme an die geänderten Löschanforderungen anzupassen, so dass Sie die Einhaltung dieser Vorgaben dokumentieren können.

Darüber hinaus erlangt der Einzelne nunmehr das Recht, seine personenbezogenen Daten in das Angebot eines anderen Anbieters übertragen zu können, „so lange der Stand der Technik dies auf verhältnismäßige Weise erlaubt.“

Auch diesbezüglich sollten Sie Ihre IT-Systeme so einrichten, dass personenbezogene Daten in gängigen elektronischen Formaten an die Betroffenen übermittelt werden können. Hierbei ist insbesondere sicherzustellen, dass bei einem Export der Daten nicht zugleich Rechte und Freiheiten Dritter beeinträchtigt werden. Der Datensatz darf daher nur personenbezogene Daten des Betroffenen, nicht aber darüber hinaus auch von Dritten enthalten. Zu diesem Zweck wird auch notwendig sein, den Betroffenen eindeutig identifizieren zu können.

5. Einwilligung in die Datenverarbeitung und Einschränkungen im Hinblick auf das Geschäftsmodell „Dienstleistung gegen Daten“

Die Einwilligung in die Datenverarbeitung soll durch eine eindeutige Handlung erfolgen, mit der ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich bekundet wird, dass die betroffene Person mit der Datenverarbeitung einverstanden ist. Es ist also stets eine „bejahende Handlung“ erforderlich. Schriftlichkeit ist nicht erforderlich, vorgekreuzte Kästchen oder Stillschweigen genügen jedoch nicht. Die Beweispflicht trifft Sie als Unternehmer.

Sonderregelungen gelten für die Anforderung an die datenschutzrechtliche Einwilligung von Kindern. Die DS-GVO sieht vor, dass Kinder ab 16 Jahren ohne nachgewiesenen Zustimmung ihre Einwilligung erteilen können. Die Mitgliedsstaaten können dieses Alter auf bis zu 13 Jahre reduzieren. Es bleibt abzuwarten, ob Deutschland von dieser Möglichkeit Gebrauch machen wird.

Einschränkungen ergeben sich durch die DS-GVO für das Geschäftsmodell „Dienstleistung gegen Daten.“ Denn die DS-GVO sieht ein sogenanntes Kopplungsverbot dergestalt vor, dass die Erbringung einer Dienstleistung nicht an die Einwilligung in die Verarbeitung personenbezogener Daten geknüpft werden darf, **wenn nicht die Erhebung der Daten zur Durchführung des Geschäfts notwendig sind.**

Es ist davon auszugehen, dass die Aufsichtsbehörden gerade diesen Punkt der Verordnung genau im Auge behalten werden. Prüfen Sie daher Ihre auf Einwilligung beruhenden Datenverarbeitungsvorgänge auch im Hinblick auf dieses Kopplungsverbot.

6. Datenaustausch im Konzern

Im Vergleich zum BDSG stellt die DS-GVO geringere Anforderungen an die Übermittlung von personenbezogenen Daten innerhalb einer Unternehmensgruppe. Aus den Erwägungsgründen zu der DS-GVO ergibt sich, dass an der Verarbeitung von personenbezogener Daten von Kunden und Beschäftigten innerhalb der Unternehmensgruppe für Verwaltungszwecke ein berechtigtes Interesse bestehen kann, dass den Datenaustausch rechtfertigt.

Auch hier sollten Sie die Prozesse allerdings so gestalten, dass die Datenübermittlung für die Betroffenen transparent ist und betroffene Mitarbeiter und Kunden informieren.

7. Der Datenschutzbeauftragte

Hinsichtlich der Pflicht zur Bestellung eines Datenschutzbeauftragten nach nationalen Vorschriften ändert sich durch die Einführung der DS-GVO im Ergebnis wenig, da die Mitgliedsstaaten in diesem Punkt von den Vorgaben der DS-GVO abweichen dürfen. Es bleibt damit bei den Regelungen des § 4f BDSG. Ein Datenschutzbeauftragter ist hiernach regelmäßig zu bestellen, wenn mehr als 9 Personen mit der Verarbeitung von personenbezogenen Daten beschäftigt sind.

Eine neue Bestellpflicht auf Grund der DS-GVO besteht allerdings dann, wenn der Fokus der Tätigkeit des Unternehmens auf der Verarbeitung von personenbezogenen Daten liegt. Hier kommt es dann auf die Mitarbeiterzahl nicht an.

8. Neuerungen betreffend die Datenschutzbehörden – One-Stop-Shop-Prinzip

Die DS-GVO statuiert bei Datenschutzverletzungen Meldepflichten gegenüber den Aufsichtsbehörden und Benachrichtigungspflichtigen gegenüber den Betroffenen. Grundsätzlich haben Sie nunmehr der Aufsichtsbehörde jede Datenschutzverletzung unverzüglich und möglichst innerhalb von 72 Stunden, nachdem Ihnen die Verletzung bekannt wurde, zu melden. Diese Pflicht entfällt, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte des Betroffenen führen wird.

Besteht hingegen ein hohes Risiko der Verletzung der Rechte des Betroffenen, so ist dieser unverzüglich von der Datenschutzverletzung in Kenntnis zu setzen.

Für Konzerne wird die Einführung des sogenannten „One-Stop-Shop-Prinzips“ relevant: Hiernach soll für eine Unternehmensgruppe und deren Töchter oder Niederlassungen jeweils nur die federführende Aufsichtsbehörde am Sitz der Hauptniederlassung zuständig sein.

9. Erweiterte Bußgeldtatbestände und höherer Bußgeldrahmen

Im Vergleich zum BDSG wird die Verletzung der vorgenannten Pflichten erheblich verschärft sanktioniert. Gegen Unternehmen können Bußgelder in Höhe von bis zu vier Prozent des globalen Umsatzes verhängt werden. Gegen Personen, die an Verstößen gegen die DS-GVO beteiligt waren, können Geldbußen in Höhe von bis zu **EUR 20.000.000,00** verhängt werden. Dies gilt auch für den Datenschutzbeauftragten! Daneben kann die zivilrechtliche Pflicht zum Schadensersatz treten.

Droht ein solches Bußgeld, können sich bestimmte Verhaltensweisen (wie etwa die Zusammenarbeit mit Aufsichtsbehörden, die Nutzung des datenschutzspezifischen Zertifizierungsverfahrens auf EU-Ebene (Art. 42 DS-GVO), oder die Einhaltung der Verhaltensregeln von Berufsverbänden oder sonstigen Interessenvertretungen), strafmildernd auswirken.

Die vorstehenden Informationen sollen Ihnen einen ersten Überblick über die Neuerungen durch die DS-GVO verschaffen, ohne dem Anspruch auf Vollständigkeit genügen zu können. Für Ihre Fragen und weitere Informationen steht Ihnen daher Ihre IHK zur Verfügung.