Das neue Datenschutzrecht - Was Unternehmen künftig zu beachten haben

Ab 25. Mai 2018 gelten in allen Mitgliedstaaten der Europäischen Union neue Datenschutzregeln. Mit der Reform soll sichergestellt werden, dass in allen Mitgliedsstaaten derselbe Datenschutzstandard besteht. Da in Deutschland bereits hohe Anforderungen an den Datenschutz gelten, führen die neuen Vorschriften zwar zu zahlreichen formellen Änderungen. Eine inhaltliche Verschärfung der Anforderungen geht mit der Reform jedoch insgesamt nicht einher.

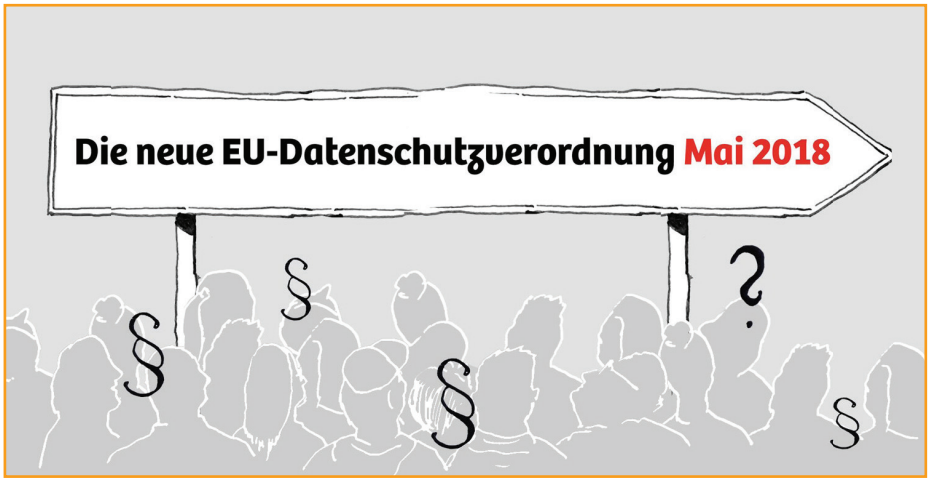
Alle Unternehmen müssen sicherstellen, dass sie bis zum 25. Mai 2018 die erforderlichen Anpassungen vornehmen. Der vorliegende Beitrag thematisiert einige der für die Praxis wichtigsten Aspekte und Fragen. Er basiert auf dem für die Mitgliedsbetriebe der Innung erstellten umfassenden Leitfaden, soll diesen aber nicht ersetzen. Er soll einen Überblick über ggf. noch zu veranlassende Maßnahmen bieten und einige Fragestellungen transparenter machen.

Anwendungsbereich der Datenschutz-Grundverordnung

Die DS-GVO (Datenschutz-Grundverordnung) gilt für die ganz oder teilweise automatische Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Sofern also eine elektronische Datenverarbeitung, auch wenn sie nur aus einem PC besteht, oder ein nach bestimmten Kriterien geordnetes Karteisystem (das können auch Karteikarten aus Papier sein) im Einsatz ist, ist der sogn. „sachliche Anwendungsbereich“ der DSGVO eröffnet.

Verarbeiten ist dabei ein umfassender Begriff für den Umgang mit personenbezogenen Daten. Er umfasst das Erheben (Daten beschaffen, sammeln), Speichern, Ändern (Berichtigung einer E-Mail-Adresse), Nutzen (Abfrage starten), Übermitteln (durch Weitergabe von Daten oder auch „reinschauen“ lassen), Verknüpfen (mit anderen Daten) oder Löschen



Bildquelle:

(einschließlich Vernichten eines Datenträgers).

Viele Unternehmer sind von den Anforderungen der DS-GVO zunächst erschlagen. Sie wissen nicht, was die DS-GVO nun konkret für sie und ihr Unternehmen bedeutet und wo sie am besten anfangen sollen. Zudem sorgen die Medienberichte der vergangenen Wochen und Monate für zusätzliche Verwirrung, zumal im Zusammenhang mit den vorgesehenen Bußgeldern bei Verstößen.

Eine einheitliche Empfehlung, die auf die Unternehmen anzuwenden ist, gibt es nicht, allerdings hat sich für die Umsetzung der neuen gesetzlichen Anforderungen in den meisten Fällen folgende Herangehensweise bewährt:

1. Bewußtmachen auf Ebene der Unternehmensleitung, dass Datenschutz Chefsache und nicht für umsonst zu haben ist.

2. Erwerb eines – aus datenschutzrechtlicher Sicht –Überblicks (Verzeichnis von Verarbeitungstätigkeiten) über Abläufe, Prozesse und Verantwortlichkeiten im Unternehmen.

3. Überprüfung, ob zur Erfüllung von Aufgaben andere Unternehmen (Auftragsdatenverarbeiter) eingeschaltet sind und falls ja, ob mit diesen für die Verarbeitung personenbezogener Daten erforderlichen Verträge abgeschlossen wurden.

4. Klarheit darüber herstellen, dass Mitarbeiter, Lieferanten, Kunden oder Interessenten, deren Daten erhoben und gespeichert wurden, sogenannte Betroffenenrechte (z. B. auf Auskunft, Berichtigung usw.) geltend machen können. Diese muss man in kurzer Zeit vollständig und richtig erfüllen können.

5. Prüfung, ob die Verarbeitung personenbezogener Daten, die im Unternehmen praktiziert wird, datenschutzrechtlich zulässig ist und ob man diese Zulässigkeit der Verarbeitung auch nachweisen kann.

6. Prüfung, ob die Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht.

Wann ist die Nutzung von Daten erlaubt?

Eine Datennutzung ist nur zulässig, wenn eine gesetzliche Vorschrift sie erlaubt oder derjenige, dessen Daten verarbeitet werden sollen, in die Nutzung von Daten einwilligt.

Vorschriften, die eine Datennutzung erlauben, finden sich hauptsächlich in Artikel 6 der Europäischen Datenschutz-Grundverordnung (DSGVO).

Diese Regelungen werden durch die §§ 22, 24, 26 des Bundesdatenschutzgesetzes (BDSG) ergänzt. Gemäß Art. 6 DSGVO ist eine Datenver-

arbeitung ohne Einwilligung zulässig, wenn

- die Verarbeitung zur Erfüllung eines Vertrags erforderlich ist (z.B. Adresse des Kunden, um den Auftrag (z. B. Anlieferung oder Abholung von Gut oder Personen ausführen zu können).
- zur Durchführung vorvertraglicher Maßnahmen erforderlich ist (z.B. E-Mail-Adresse, um dem Kunden nach seinem Wunsch einen Kostenvoranschlag (z. B. Umzugsangebot, Transportanfrage oder Reiseanfrage senden zu können).
- zur Wahrung berechtigter Interessen des Unternehmens oder eines Dritten erforderlich ist und die Interessen der betroffenen Person nicht überwiegen (z.B. die Auswertung der Kundendatei, um bestimmte Kunden zielgerichtet mit Werbung anzusprechen).

Die Verarbeitung personenbezogener Daten von Arbeitnehmern konkretisiert § 26 BDSG. Hiernach ist eine Verarbeitung zulässig, wenn es

- zur Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist (z.B. Speicherung von Lohnunterlagen und Krankheitstagen).
- zur Ausübung der Interessensvertretung der Beschäftigten erforderlich ist

Anforderungen der datenschutzrechtlichen Einwilligung

Eine Datennutzung ist – wie bereits ausgeführt - nur zulässig, wenn eine gesetzliche Vorschrift sie erlaubt oder derjenige, dessen Daten verarbeitet werden sollen, in die Datennutzung einwilligt.

Eine rechtmäßige Datennutzung setzt deshalb entweder eine gesetzliche Erlaubnis oder eine Einwilligung des Betroffenen voraus. Damit eine Einwilligung wirksam ist, müssen die gesetzlichen Anforderungen an eine Einwilligungserklärung erfüllt sein. Für Unternehmen gelten die Vorschriften der Europäischen Datenschutzgrundverordnung (Artikel 7 DSGVO), die durch das Bundesdatenschutzgesetz (§ 51 BDSG) ergänzt werden.

Eine Einwilligung ist nur dann rechtmäßig, wenn derjenige, der die Einwilligung erklärt, dies freiwillig tut. Jede Form von Druck, Zwang oder Verpflichtung führt deshalb zur Unwirksamkeit der Einwilligung. Eine Einwilligung gilt unter anderem bereits als unfreiwillig, wenn der Abschluss eines Vertrags oder die Erbringung einer Leistung von der Abgabe der Einwilligungserklärung abhängig gemacht wird und der Kunde keine Möglichkeit hat, die Leistung auf andere Weise zu erlangen. Die Wirksamkeit einer Einwilligung ist nicht vom Alter des Einwilligenden abhängig. Insofern spielt es an sich keine Rolle, ob es sich um einen Minderjährigen oder einen Volljährigen handelt. Für die Wirksamkeit der Einwilligung ist allein die Einsichtsfähigkeit des Einwilligenden in die Tragweite seiner Erklärung maßgeblich. Der Einwilligende muss erkennen können, welche Folgen die Einwilligung für ihn hat.

Ob Minderjährige diese Einsichtsfähigkeit besitzen, kann nicht pauschal beurteilt werden, sondern richtet sich nach den Umständen des Einzelfalls. Da die Einsichtsfähigkeit eines Minderjährigen nicht in jedem Fall mit abschließender Sicherheit beurteilt werden kann, empfiehlt es sich in der Praxis, bei Minderjährigen stets die Einwilligungserklärung der Erziehungsberechtigten einzuholen.

Einwilligungen müssen – anders als früher – nicht mehr schriftlich erklärt werden. Eine mündliche Einwilligung ist deshalb in gleicher Weise wirksam. Allerdings sollte die Einwilligungserklärung allein aus Beweis- und Dokumentationsgründen stets in Textform eingeholt werden. Die gewählte Form der Einwilligung ist zugleich Maßstab für den Fall, dass die Einwilligung widerrufen wird. Wurde die Einwilligung mündlich erteilt, muss ein mündlich erklärter Widerruf akzeptiert werden. Die Dokumentation mündlicher Erklärungen ist allerdings aufwändig, fehleranfällig und für effiziente Betriebsabläufe nicht zu empfehlen. Die gesetzlichen Vorschriften geben klare Mindestanforderungen an Einwilligungen vor. Die Angaben müssen verständlich und in klarer, einfacher Sprache formuliert werden. Sie müssen so konkret und so umfassend sein, dass sich der Einwilligende darüber ein Bild machen kann, was mit seinen Daten passiert.

Die Einwilligungserklärung ist optisch so zu gestalten, dass sie ins Auge fällt und vom Einwilligenden wahrgenommen wird. Dies ist vor allem dann wichtig, wenn die Einwilligungserklärung zusammen mit anderen Informationen (z.B. Allgemeinen Geschäftsbedingungen) in einem einzigen Text vorgelegt wird. Die erforderliche optische Abhebung ist beispielsweise durch eine Einrahmung, einen Fettdruck, eine andere Farbe oder durch eine andere Schriftgröße möglich.

Die Einwilligung muss aktiv erklärt werden und sollte durch eine eindeutige bestätigende Handlung erfolgen.

Beachte:

Die Datennutzung zur Direktwerbung ist zulässig. Allerdings dürfen Betroffene der Werbung jederzeit widersprechen (Art. 21 Absatz 2 DSGVO). Für Werbung per E-Mail ist weiterhin eine Einwilligung erforderlich. Soll die datenschutzrechtliche Einwilligung gemeinsam mit weiteren Erklärungen abgegeben werden, so sollte für jede Erklärung eine gesonderte Unterzeichnung oder ein gesondertes Anklicken vorgesehen werden.

Dies bietet sich allein aus Beweiszwecken an. Obwohl die gesetzlichen Vorschriften keine zeitliche Geltungsdauer vorsehen, wird in der Praxis davon ausgegangen, dass erklärte Einwilligungen nicht unbeschränkt gültig sind. Eine Einwilligung kann nur herangezogen werden, solange derjenige, der eingewilligt hat, vernünftiger Weise mit einer Verarbeitung seiner Daten rechnen muss. Dies kann je nach Fall unterschiedlich sein. Wer seine Einwilligung zum Erhalt von Werbung zu den regelmäßigen Sonderaktionen z. B. eines Autovermieters erklärt hat, muss nicht damit rechnen, dass er nach mehreren Jahren erstmals oder erneut Werbung erhält.

Formelle Pflichten von Unternehmen – Ein Überblick

Das Datenschutzrecht räumt Personen, deren Daten von Unternehmen genutzt werden, zahlreiche Rechte ein. Mithilfe dieser Rechte soll erreicht werden, dass diese Betroffenen Einfluss auf den Umgang und die Verbreitung ihrer Daten haben.

Für Unternehmen, die Daten verarbeiten, bestehen andererseits gewisse Anforderungen an die Datennutzung. Wer Daten z.B. seiner Kunden und Geschäftspartner nutzen möchte, muss diese überwiegend formalen Anforderungen erfüllen. Die Pflichten von Unternehmen und die Rechte von Betroffenen sind in den Artikeln 12 bis 22 der Datenschutz-Grundverordnung (DSGVO) geregelt. Die Vorschriften werden durch die §§ 32 bis 37 des Bundesdatenschutzgesetzes (BDSG) ergänzt.

Unternehmen, die Daten nutzen, werden vom Gesetz als „Verantwortliche“ bezeichnet, weil sie die Datennutzung verantworten und für Datenpannen einstehen müssen.

Die Pflichten sind im Einzelnen:

- ***Transparenzgebot (Art. 12 DSGVO)***

  Art. 12 regelt den Umgang mit Anfragen des Betroffenen und in welcher Form Anfragen zu beantworten sind. Der Verantwortliche hat der betroffenen Person sämtliche Informationen und alle Mitteilungen auf präzise, transparente, verständliche und leicht zugängliche Weise in einer klaren und einfachen Sprache unverzüglich zu übermitteln. Obwohl auch eine mündliche Information zulässig ist, ist in der Praxis die Textform allein aus Beweisgründen zu empfehlen. Hierbei spielt es keine Rolle, ob der Text in Papierform oder elektronisch übermittelt wird.

- ***Informationspflichten (Art. 13 und 14 DSGVO)***

  Art. 13 regelt, welche Informationen der Verantwortliche dem Betroffenen zu erteilen hat, wenn er beim Betroffenen Daten erhebt. Art. 14 bestimmt die Informationspflichten, wenn die Daten nicht bei der betroffenen Person selbst, sondern bei einem Dritten erhoben werden.

- ***Auskunftsrecht (Art. 15 DSGVO)***

  Betroffene haben das Recht, vom datenverarbeitenden Betrieb eine Bestätigung zu verlangen, ob über sie personenbezogene Daten gespeichert sind und verarbeitet werden. Ist das der Fall, hat der Betrieb Auskunft über diese Daten, deren Herkunft sowie weitere Informationen zu erteilen. In der Praxis werden solche Auskunftsanfragen i.d.R. von Kunden auf Unternehmen. Denkbar wäre allerdings auch, dass z. B. Mitarbeiter Informationen darüber haben möchten, welche Daten vom Unternehmen gespeichert werden bzw. wurden und an wen ggf. eine Weitergabe ihrer Beschäftigungsdaten erfolgt ist.

- ***Recht auf Berichtigung (Art. 16 DSGVO)***

  Sind personenbezogene Daten falsch, nicht mehr aktuell oder unvollständig, haben die betroffenen Personen gemäß Art. 16 ein Recht auf Berichtigung. Der verantwortliche Datenverarbeiter (das Unternehmen) muss die unrichtigen oder unvollständigen Daten unverzüglich korrigieren.

- ***Recht auf Löschung (Art. 17 DSGVO)***

  Nach Art. 17 haben Betroffene das Recht, die Löschung ihrer Daten zu verlangen, wenn einer der gesetzlich geregelten Löschungsgründe vorliegt. Ein solcher Grund liegt vor, wenn:

  - die Aufbewahrung der Daten für den Zweck, zu dem sie ursprünglich erhoben wurden, nicht mehr erforderlich ist,
  - die Daten unrechtmäßig verarbeitet wurden,
  - der Betroffene seine Einwilligung für eine weitere Speicherung widerrufen hat.

  Selbst wenn einer der vorgenannten Gründe vorliegt, dürfen Daten aber nicht gelöscht werden, wenn gesetzliche Aufbewahrungsfristen bestehen und der Verantwortliche damit zur Aufbewahrung verpflichtet ist (z.B. bei rentenrelevanten Unterlagen von Mitarbeitern oder Arbeitszeitaufzeichnungen gemäß Mindestlohngesetz oder wenn diese für die Lohnabrechnung benötigt wurden).

  Anstelle einer Löschung tritt die sog. Einschränkung der Verarbeitung gemäß § 35 BDSG, wenn die Löschung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Interesse des Betroffenen an der Löschung als gering anzusehen ist.

- ***Recht auf Vergessenwerden (Art. 17 DSGVO)***

  Eine besondere Form des Löschungsanspruchs ist das „Recht auf Vergessenwerden“. Dieses Recht bezieht sich auf Daten, die veröffentlicht wurden und zielt insbesondere auf Veröffentlichungen im Internet ab. Für die Mitgliedsbetriebe der Innung dürfte dies in der Praxis jedoch keine große Rolle spielen

- ***Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)***

  Mit dem Recht auf Einschränkung der Verarbeitung können Betroffene in bestimmten Fällen erwirken, dass der Datenverarbeiter ihre Daten sperrt und somit nicht weiter verarbeiten darf.

  Dies gilt u.a. für den Fall, dass die Richtigkeit gespeicherter Daten bestritten wird und die Datennutzung für die Dauer der Überprüfung der Richtigkeit ausgesetzt werden soll, die Datenverarbeitung unrechtmäßig ist und der Betroffene anstatt der Löschung die Nutzungseinschränkung bevorzugt.

❖

Pflicht zur Datenübertragung (Art. 20 DSGVO)

Das Recht auf Datenübertragung gibt Betroffenen unter bestimmten Voraussetzungen einen Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen Dateiformat zu erhalten (z. B. eine Excel-Tabelle). Der Betroffene hat damit das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen". Die Regelung soll den Wechsel zu einem anderen Anbieter insbesondere bei sozialen Netzwerken oder Verträgen mit Energieversorgern, Banken und Versicherungen erleichtern.

❖

Widerspruchsrecht (Art. 21 DS-GVO)

Betroffenen steht ein Widerspruchsrecht gegen eine Verarbeitung ihrer Daten zum Zweck der Direktwerbung zu. Obwohl die Nutzung von Daten zur Direktwerbung zulässig ist, können betroffene Personen hiergegen jederzeit und ohne Angabe von Gründen widersprechen.

Nach erfolgtem Widerspruch dürfen die Daten nicht mehr zur Direktwerbung genutzt werden.

❖

Dokumentationspflicht (Art. 30 DSGVO)

Alle Unternehmen sind verpflichtet, sämtliche Verarbeitungsprozesse im sogenannten „Verzeichnis von Verarbeitungstätigkeiten" zu dokumentieren. Hierdurch soll eine Übersicht über die datenschutzrelevanten Abläufe im Betrieb gegeben werden. Erweist sich eine beabsichtigte Datennutzung als risikoreich, ist zusätzlich eine „Datenschutz-Folgenabschätzung" nach Art. 35 DSGVO vorzunehmen.

Informationspflichten bei Erhebung personenbezogener Daten

Personen, deren Daten von einem anderen verarbeitet werden, sollen im Vorlauf zur Datenverarbeitung informiert werden. Insbesondere sollen sie erfahren, welche Daten über sie erhoben und zu welchem Zweck sie genutzt werden. Um diese Transparenz herzustellen, sind Unternehmen verpflichtet, den jeweils betroffenen Personen zahlreiche Informationen über die beabsichtigte Datennutzung zu erteilen.

Welche Informationen dies im Einzelnen sind, ist in den Art. 13 und 14 der Europäischen Datenschutz-Grundverordnung (DSGVO) aufgelistet, die durch §§ 32 und 33 des Bundesdatenschutzgesetzes (BDSG) ergänzt werden.

Bei den Informationspflichten sind drei Situationen zu unterscheiden:

- Die Daten werden bei der Person, deren Daten verarbeitet werden sollen, direkt erhoben. (z. B. wenn einer neuer Kunde direkt in Kontakt mit einem Anbieter tritt.)

- Die Daten, die verarbeitet werden sollen, werden nicht bei der betroffenen Person selbst, sondern von einem Dritten erhoben. (z. B. bei Aufträgen von Paketdienstleistern o. a.)

Der Datenverarbeiter hat die Daten bereits vorliegen und möchte die Daten zu einem anderen Zweck nutzen, als zu dem, zu dem sie ursprünglich bei der betroffenen Person erhoben wurden.(z. B. wenn ein Umzugsunternehmen z. B. noch eine Autovermietung betreibt und den Umzugskunden hierfür Werbung zukommen lässt).

Im Fall der Datenerhebung beim Betroffenen müssen die Informationen im Zeitpunkt der Datenerhebung mitgeteilt werden. Werden die Daten nicht beim Betroffenen erhoben, muss der Verantwortliche die Informationen innerhalb einer angemessenen Frist, spätestens jedoch nach einem Monat erteilen. Bei einer Zweckänderung ist der Betroffene vor der Verwendung der Daten zum neuen Zweck zu unterrichten.

Die Information des Betroffenen ist nicht erforderlich, soweit dieser bereits Kenntnis über die einzelnen Angaben der Datenverarbeitung hat. Werden die Daten bei einem Dritten erhoben, darf die Information zudem unterbleiben, wenn die Informationserteilung unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.

Neben den Informationspflichten unterliegen datenverarbeitende Unternehmen auch breiten Auskunftspflichten gegenüber Betroffenen. Auf diese soll im Rahmen des vorliegenden Beitrags nicht eingegangen werden, detaillierte Informationen sind jedoch im Innungsleitfaden enthalten.

Dokumentationspflichten

Alle Unternehmen, die personenbezogene Daten verarbeiten, sind verpflichtet, sämtliche Verarbeitungsprozesse im sogenannten „Verzeichnis von Verarbeitungstätigkeiten" zu dokumentieren. Hierdurch soll eine Übersicht über die datenschutzrelevanten Abläufe im Betrieb gegeben werden. Auf Grundlage dieser Übersicht sollen sich Betriebsinhaber über das Ausmaß und die Intensität der betrieblichen Datenverarbeitung bewusst werden.

Die Pflicht zur Dokumentation der Datenverarbeitungsprozesse sowie die konkreten Anforderungen an die Dokumentation sind in Artikel 30 der Europäischen Datenschutz-Grundverordnung (DSGVO) geregelt.

Danach sind alle Tätigkeiten zu dokumentieren, bei denen personenbezogene Daten verarbeitet werden. Solche Tätigkeiten können in den unterschiedlichsten betrieblichen Situationen vorkommen (z.B. Erstellung und Veränderung der Kundendatei, Verwaltung der Mitarbeiterakten, Verwendung einer Kamera im Betrieb).

Es sei an dieser Stelle darauf verwiesen, dass zwar alle Tätigkeiten dokumentiert werden sollen, allerdings nur exemplarisch wie z. B. Erstellung und Veränderung der Kundendatei. Art. 30 DS-GVO meint explizit nicht, dass jeden Tag alle Vorgänge, in denen personenbezogene Daten verarbei-

tet werden, in dem Verzeichnis von Verarbeitungstätigkeiten eingetragen werden sollen.

Das Verzeichnis ist nicht öffentlich. Es muss also insbesondere betroffenen Personen, wenn diese Einblick in die Verarbeitung der sie betreffenden personenbezogenen Daten fordern, nicht offengelegt werden.

Es dient neben der eigenen Qualitätskontrolle ausschließlich dafür, der Aufsichtsbehörde nachzuweisen, in welchem Verfahren in dem jeweiligen Unternehmen mit personenbezogenen Daten umgegangen wird. Es kann auch, wenn es nicht auf den Minimalinhalt beschränkt wird, als Nachweis für die Einhaltung weiterer Datenschutzvorschriften dienen.

Der betriebliche Datenschutzbeauftragte (DSB)

Sind im Betrieb mindestens 10 Personen angestellt, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ist ein DSB zu benennen.

Als automatisierte Verarbeitung gelten z.B.:

- Nutzung digitaler Kundendateien.
- Verwendung von Kundendaten auf einem Tablet- PC, Smartphone oder einem anderen mobilen Endgerät.

Für mehrere Standorte bzw. Filialen kann ein einziger DSB bestellt werden. Hierbei ist zu beachten, dass die Anzahl der Filialen nur so hoch sein darf, dass der DSB seine Aufgaben in jeder Filiale realistisch erfüllen kann. Wenn das Gesetz für ein Unternehmen die Benennung eines DSB nicht vorschreibt, sollte überlegt werden, ob freiwillig ein DSB benannt wird. Dies ist nach dem Gesetz ausdrücklich möglich.

Der DSB kann sowohl ein Mitarbeiter des Betriebs (interner DSB) oder ein außenstehender Dienstleister (externer DSB) sein. Unabhängig davon, ob es sich um einen internen oder externen DSB handelt, dürfen nur solche Personen bestellt werden, die fachliche Qualifikationen auf dem Gebiet des Datenschutzes besitzen (Datenschutzrecht und IT-Fachwissen) und bei der Aufgabenwahrnehmung in keinen Interessenskonflikt geraten können (Interessenskonflikte bestehen z.B. für Mitglieder der Geschäftsführung, Leiter der EDV oder der Personalabteilung, etc., da diese Personen für die Datenverarbeitung verantwortlich sind und sich als DSB selbst kontrollieren würden).

Nach der Bestellung sind jedoch neue Informationspflichten zu beachten:

- Die Kontaktdaten des DSB (z.B. E-Mail-Adresse, Durchwahlnummer, etc.) sind zu veröffentlichen (z.B. auf der Webseite des Betriebs).
- Die Kontaktdaten des DSB sind der jeweiligen Landesdatenschutzbehörde zu melden.

Wichtig ist, dass nur über die Kontaktdaten zu informieren ist. Dies umfasst nicht zwingend den Namen des DSB.

Sanktionen bei Verstößen

Verstöße gegen den Datenschutz können ernsthafte rechtliche Folgen nach sich ziehen. Die DS-GVO hat die bisher geltenden Regelungen deutlich verschärft. Dies gilt sowohl im Hinblick auf denkbare Geldbußen als auch im Hinblick auf Schadensersatz einschließlich Schmerzensgeld. Die DS-GVO enthält Bestimmungen für Geldbußen und Bestimmungen für das Recht auf Schadensersatz einschließlich Schmerzensgeld.

Abschließend sei für Mitgliedsbetriebe der Innung nochmals ausdrücklich auf den Ende März verbandsintern veröffentlichten Leitfaden verwiesen, der deutlich umfassender, als es der vorliegende Beitrag leisten kann, informiert und mit Checklisten, Formularvorschlägen und Mustern die Umsetzung der DS-GVO in der betrieblichen Praxis deutlich erweitert. Zudem bietet die Wirtschaftsorganisation der Innung, die FGIBB Service GmbH im sowohl im Juni als auch im August ein dreitägiges Seminar mit Prüfung) zur Qualifikation interner DSB an.

Informationen hierzu sind auf der Homepage der FGIBB Service GmbH (im Kalender) oder telefonisch (030-2529 5010) erhältlich.

Seminarhinweis

Juni

Freitag, 15. Juni 2018 in der Zeit von 12:00 bis 17:00 Uhr

Samstag, 16. Juni 2018 in der Zeit von 08:00 bis 16:00 Uhr

Samstag, 23. Juni 2018 in der Zeit von 08:00 bis 12:00 Uhr

anschließend Prüfung in der Zeit von 12:30 - 13:30 Uhr

August

Mittwoch, 29. August 2018 in der Zeit von 08:00 bis 16:00 Uhr

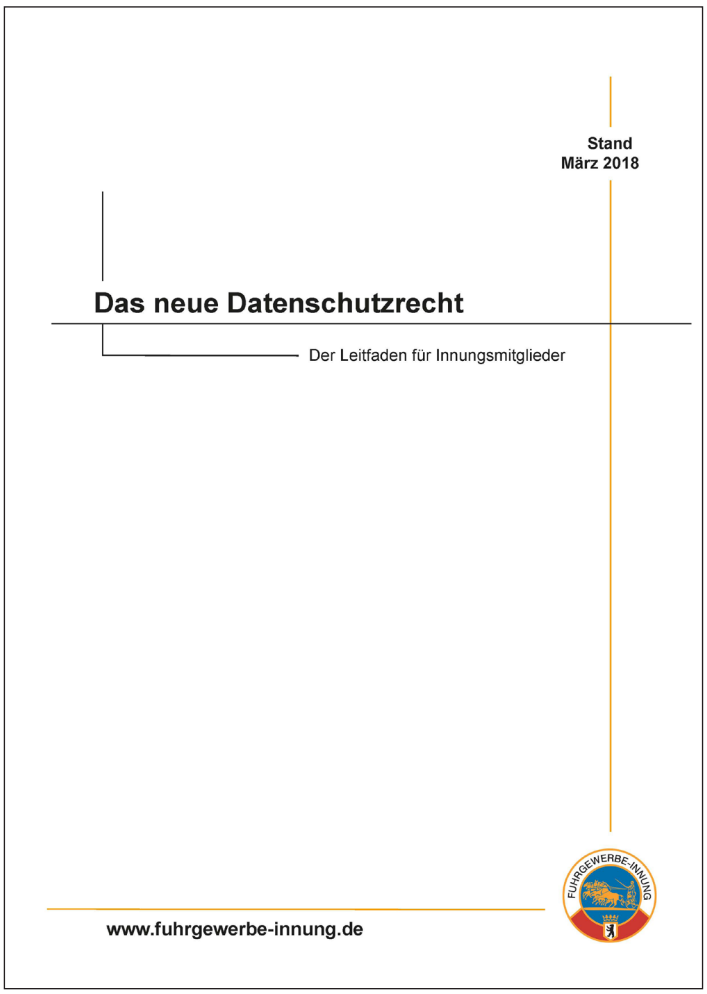
Donnerstag, 30. August 2018 in der Zeit von 08:00 bis 16:00 Uhr

Freitag, 31. August 2018 in der Zeit von 08:00 bis 12:00 Uhr

anschließend Prüfung in der Zeit von 12:30 - 13:30 Uhr

Es wird eine Teilnahmegebühr in Höhe von **850,00 € netto** zzgl. 19 % MwSt pro Teilnehmer aus Innungsbetrieben fällig.

Für Teilnehmer aus **Nicht-Mitgliedsbetrieben beträgt die Teilnahmegebühr 900,00 €** pro Teilnehmer. In den Kosten sind Lehrmaterialien, Imbiss sowie Tagungsgetränke enthalten.



Der Leitfaden nebst der 18 Anlagen steht allen Mitgliedern im geschützen Bereich auf der Innungshomepage unter dem Bereich „Allgemeines“ zur Verfügung.

Die Mitglieder der Fuhrgewerbe-Innung erhielten in der 17. Kalenderwoche auf dem Postweg jeweils ein Exemplar zu Ihrer Verwendung.

ANMELDUNG

Bitte bis spätestens **10. Mai 2018** zurücksenden!

Per Telefax: 030/25 29 50 11

FGIBB Service GmbH
Hedemannstraße 13
10969 Berlin

Rechnungsanschrift

Grundlehrgang
„Betrieblicher Datenschutzbeauftragter nach Bundesdatenschutzgesetz“

Sie haben in diesem Seminar die Möglichkeit, nach BDSG und EU-DSGVO erforderliche Fachkunde für betriebliche Datenschutzbeauftragte zu erwerben. Es liefert Ihnen die zur Ausübung Ihrer Tätigkeit notwendigen Grundlagen und vermittelt aktuelles Wissen zum Datenschutzgesetz; deshalb eignet es sich gleichermaßen für neubestellte wie bereits tätige Datenschutzbeauftragte.

TERMINE
Freitag, 15. Juni 2018 in der Zeit von 12:00 bis 17:00 Uhr
Samstag, 16. Juni 2018 in der Zeit von 08:00 bis 16:00 Uhr
Samstag, 23. Juni 2018 in der Zeit von 08:00 bis 12:00 Uhr
anschließend Prüfung in der Zeit von 12:30 - 14:30 Uhr

Ich melde mich verbindlich für die Teilnahme am o. g. Seminar bei der FGIBB Service GmbH an.

Name, Vorname des Teilnehmers: _____ geb. am: _____

derzeitige Tätigkeit: _____

Name und Anschrift des Unternehmens: _____

Telefon: _____ Fax: _____

Von den umseitigen Teilnahmebedingungen habe ich Kenntnis genommen.

Teilnahmegebühr:
Es wird eine Teilnahmegebühr in Höhe von **850,00 € netto zzgl. 19 % MwSt** pro Teilnehmer aus Innungsbetrieben fällig. Für Teilnehmer aus Nicht-Mitgliedsbetrieben beträgt die Teilnahmegebühr 900,00 € pro Teilnehmer. In den Kosten sind Lehrmaterialien, Imbiss sowie Tagungsgetränke enthalten.

Datum _____ Unterschrift _____

FGIBB Service GmbH
Hedemannstraße 13
10969 Berlin
Telefon: 030 25 29 50 10
Telefax: 030 25 29 50 11
E-Mail: post@fgibb.de
Internet: www.fgibb.de

Melden Sie sich über den QR-Code direkt zu den Seminaren an.

ANMELDUNG

Bitte bis spätestens **31. Juli 2018** zurücksenden!

Per Telefax: 030/25 29 50 11

FGIBB Service GmbH
Hedemannstraße 13
10969 Berlin

Rechnungsanschrift

Grundlehrgang
„Betrieblicher Datenschutzbeauftragter nach Bundesdatenschutzgesetz“

Sie haben in diesem Seminar die Möglichkeit, nach BDSG und EU-DSGVO erforderliche Fachkunde für betriebliche Datenschutzbeauftragte zu erwerben. Es liefert Ihnen die zur Ausübung Ihrer Tätigkeit notwendigen Grundlagen und vermittelt aktuelles Wissen zum Datenschutzgesetz; deshalb eignet es sich gleichermaßen für neubestellte wie bereits tätige Datenschutzbeauftragte.

TERMINE
Mittwoch, 29. August 2018 in der Zeit von 08:00 bis 16:00 Uhr
Donnerstag, 30. August 2018 in der Zeit von 08:00 bis 16:00 Uhr
Freitag, 31. August 2018 in der Zeit von 08:00 bis 12:00 Uhr
anschließend Prüfung in der Zeit von 12:30 - 13:30 Uhr

Ich melde mich verbindlich für die Teilnahme am o. g. Seminar bei der FGIBB Service GmbH an.

Name, Vorname des Teilnehmers: _____ geb. am: _____

derzeitige Tätigkeit: _____

Name und Anschrift des Unternehmens: _____

Telefon: _____ Fax: _____

Von den umseitigen Teilnahmebedingungen habe ich Kenntnis genommen.

Teilnahmegebühr:
Es wird eine Teilnahmegebühr in Höhe von **850,00 € netto zzgl. 19 % MwSt** pro Teilnehmer aus Innungsbetrieben fällig. Für Teilnehmer aus Nicht-Mitgliedsbetrieben beträgt die Teilnahmegebühr 900,00 € pro Teilnehmer. In den Kosten sind Lehrmaterialien, Imbiss sowie Tagungsgetränke enthalten.

Datum _____ Unterschrift _____

FGIBB Service GmbH
Hedemannstraße 13
10969 Berlin
Telefon: 030 25 29 50 10
Telefax: 030 25 29 50 11
E-Mail: post@fgibb.de
Internet: www.fgibb.de