# Merkblatt Datenschutz
# 2018

erstellt von dl-DATEN GmbH | Hoher Holzweg 17 | 30966 Hemmingen

Inhaltsübersicht

## EINFÜHRUNG:

Sehr geehrte Damen, sehr geehrte Herren,

egal ob Sie mit Daten der Kunden, der Mitarbeiter oder sonstigen personenbezogenen Daten Ihres Unternehmens umgehen – es geht um den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

Seit dem 25.Mai 2018 gilt ein neues in den Grundzügen europaweit einheitliches Datenschutzrecht in Form der DatenSchutzGrundVerOrndnung (DSGVO).

In Deutschland tritt zu diesem Zeitpunkt das auf dieses europäische Recht abgestimmte neue BundesDatenSchutzGesetz (BDSGneu) in Kraft.

Das Merkblatt soll einen Überblick über die Grundlagen des (neuen) Datenschutzes geben und über Ihre Rechte und Pflichten aufklären.

Wir als Dienstleister im Bereich Datenschutz und IT-Sicherheit stehen Ihnen mit unserem Team selbstverständlich in allen Zweifelsfragen zur Verfügung.

Bitte nutzen Sie die Möglichkeit.

dl-DATEN GmbH | Hoher Holzweg 17 | 30966 Hemmingen

Telefon: +49 511 536770-80 | Fax: +49 511 536770-88 | E-Mail: datenschutz@dl-daten.de | www.dl-daten.de

## GRUNDREGEL DES DATENSCHUTZRECHTS

Das Verarbeiten personenbezogener Daten ist grundsätzlich verboten!

Personenbezogene Daten sind nach Art. 4 Nr.1 DSGVO

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Dies umfasst z. B. Name, Geburtsdatum, Anschrift, Einkommen, Beruf, Kfz-Kennzeichen, Konto- oder Versicherungsnummer. Auch pseudonymisierte Daten, zum Beispiel eine IP-Adresse oder Personalnummer, aus denen die betroffene Person indirekt bestimmbar wird, gelten als personenbezogene Daten.

Sehr vereinfacht ließe sich dies wie folgt zusammenfassen: Name und (nahezu jegliche) zusätzliche Angabe/Information

## Verarbeiten

ist jedes mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie

- das Erheben, das Erfassen,
- die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung,
- das Auslesen, das Abfragen, die Verwendung,
- die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,
- die Einschränkung,
- das Löschen oder die Vernichtung, wiederum sehr vereinfacht also alles vom Erheben über Lesen bis zum Löschen.

Der Gesetzgeber regelt wann (und zu welchem Zweck) das Verarbeiten personenbezogener Daten überhaupt nur erlaubt ist und stellt gleichzeitig Regeln auf, die bei der Verarbeitung zu berücksichtigen sind.

Die Verarbeitung besonderer Kategorien personenbezogener Daten, aus denen

die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist nur unter besonderen ganz eingeschränkten Voraussetzungen zugelassen.

Erlaubt ist die Verarbeitung (Art. 6 Abs. 1 DSGVO), u.a. wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Erlaubt ist die Verarbeitung (zusätzlich gemäß § 26ff. BDSGneu), u.a. und unter besonderen Voraussetzungen, wenn

- für Zwecke des Beschäftigungsverhältnisses,sogar die Verarbeitung besonderer Kategorien personenbezogener Daten
- zu im öffentlichen Interesse liegenden Archivzwecken,
- für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke.

Ist die Verarbeitung personenbezogener Daten grundsätzlich zulässig sind u.a. folgende wesentliche Regeln einzuhalten:

- Verarbeitung nach Treu und Glauben,
- Zweckbindung,
- Datensparsamkeit,
- Richtigkeit der Daten,
- Begrenzung der Speicherdauer,
- Transparenz,
- Berücksichtigung des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sowie
- „Integrität und
- Vertraulichkeit" der Datenverarbeitung; so dürfen mit der Datenverarbeitung befasste Personen personenbezogene Daten nicht unbefugt verarbeiten und sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

Technisch-organisatorische Maßnahmen sind zu treffen, die die Sicherheit der Verarbeitung gewährleisten, Art. 32 DSGVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; etwa:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind. Dies insbesondere durch Vernichtung, Verlust oder Veränderung (ob unbeabsichtigt oder unrechtmäßig) oder unbefugte Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

präzisiert diese Anforderungen an die Sicherheit der Datenverarbeitung.

Der Verantwortliche und der Auftragsverarbeiter haben auch die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

Im Fall einer automatisierten Verarbeitung haben (in teilweiser Änderung zur geltenden Anlage zu § 9 BDSG) der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

- Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (**Zugangskontrolle)**,
- Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (**Datenträgerkontrolle**),
- Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (**Speicherkontrolle**),
- Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (**Benutzerkontrolle**),
- Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (**Zugriffskontrolle**),
- Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle**),
- Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (**Eingabekontrolle**),
- Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (**Transportkontrolle**),
- Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellbarkeit**),
- Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (**Zuverlässigkeit)**,
- Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**),
- Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
- Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
- Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (**Trennbarkeit**).

Dies kann zum Teil auch durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

WESENTLICHE NEUERUNGEN DURCH DSGVO UND BDSGNEU AB MAI 2018:

## 1. Räumlicher Anwendungsbereich – das Marktortprinzip

Die DSGVO stellt für ihre räumliche Geltung nicht mehr auf den Sitz eines Unternehmens ab, sondern darauf, ob ein Anbieter von entgeltlichen oder unentgeltlichen Waren oder Dienstleistungen personenbezogene Daten von in der EU befindlichen Personen verarbeitet.

Daneben ist die DSGVO auch dann anzuwenden, wenn die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient. Unter Letzteres fällt die Analyse des Surfverhaltens im Internet und auch die Speicherung von Cookies, egal zu welchem Zweck (Art. 3 Abs. 2 DSGVO).

## 2. Grundsätze der Datenverarbeitung

An den Grundsätzen der Datenverarbeitung wurde im Kern nichts geändert. In Art. 5 DSGVO werden die bekannten Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, der Zweckbindung, der Datensparsamkeit, der Richtigkeit, der Begrenzung der Speicherdauer genannt und durch die „Integrität und Vertraulichkeit" der Datenverarbeitung ergänzt. Die Zweckbindung wird dadurch gestärkt, dass sie nun durch die Verordnung ohne Abweichungsmöglichkeit der Mitgliedstaaten verbindlich ist und die Betroffenen nun vor Zweckänderungen der Datennutzungen informiert werden müssen. Die Nutzung von zweckgebunden erhobenen Daten zu einem mit dem ursprünglichen Erhebungszweck unvereinbaren Zweck ist nicht zulässig. Für eine solche Zweckänderung müssen die Daten also auf rechtmäßigem Weg erneut erhoben werden.

## 3. Verzeichnis aller Datenverarbeitungstätigkeiten

Art. 30 DSGVO ordnet an, dass Verantwortliche und Auftragsdatenverarbeiter ein Verzeichnis über alle Verarbeitungstätigkeiten unter der Angabe der im Artikel genannten Punkte führen müssen. Dieses Verzeichnis ist nach Anfrage der Aufsichtsbehörde zur Verfügung zu stellen. Die vorgesehene Grenze von Unternehmen von zumindest 250 Mitarbeitern läuft dabei faktisch-praktisch ins Leere; auf der einen Seite ist das Nichtvorhalten eines solchen Verzeichnisses trotz Verpflichtung mit erheblichen Bußgeldern bedroht, andererseits wird allein schon die Tatsache, dass eine Krankschreibung vorliegt als „besondere Kategorie personenbezogener Daten" gewertet, deren Verarbeitung die Grenze entfallen lässt.

## 4. Erweiterung der Informationspflichten und Transparenz

Um die Verwendung von Daten nachvollziehbar zu machen wurden die Informationspflichten der Daten Verarbeiter gegenüber den Betroffenen in Art. 14 und 15 DSGVO erheblich erweitert.

Der Betroffene ist vor Erhebung von personenbezogenen Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache über die in den Artikeln genannten Verwendungsgesichtspunkte zu informieren. Im Einzelnen sind dies:

- Name und Kontaktdaten des für die Datenerhebung Verantwortlichen,
- die Kontaktdaten des Datenschutzbeauftragten,
- die Zwecke und die Rechtsgrundlage der Verarbeitung,
- das berechtigte Interesse des Verantwortlichen oder eines Dritten,
- Empfänger der personenbezogenen Daten,
- die Absicht der Übermittlung an ein Drittland oder eine internationale Organisation.
- Daneben ist der Betroffene auch über
- die voraussichtliche Dauer der Datennutzung,
- die betroffenen Rechte auf Auskunft, Berichtigung, Löschung und eventuelle Einschränkungen dieser Rechte,
- das Recht auf jederzeitigen Widerruf der Einwilligung,
- das Beschwerderecht bei einer Aufsichtsbehörde,
- die Bereitstellung der personenbezogenen Daten,
- eine automatische Entscheidungsfindung zu informieren.

Falls die Daten nicht vom Betroffenen stammen, ist dieser in gleicher Weise zu informieren und darüber hinaus über die Quelle seiner Daten in Kenntnis zu setzen.

Diese strengen Transparenzvorgaben gelten auch für die Einwilligung, die durch eine eindeutige Handlung erfolgen muss und mit der die betroffene Person ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich erklärt, dass sie mit der Verarbeitung ihrer Daten einverstanden ist. Gerade bei komplexeren Sachverhalten muss das Ersuchen um eine Einwilligung „in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" erfolgen.

Ein Vertragsschluss darf nicht davon abhängig gemacht werden, dass die betroffene Person eine Einwilligung in die Verarbeitung personenbezogener Daten abgibt, die für die Erfüllung des Vertrags nicht erforderlich sind (Koppelungsverbot). Zudem können Einwilligungen jederzeit beliebig widerrufen werden.

## 5. „Recht auf Vergessenwerden, Art. 17"

Verlangt der Betroffene die Löschung, ist der Verantwortliche verpflichtet die Löschung unter den vorgeschriebenen Voraussetzungen unverzüglich vorzunehmen. Wurden die personenbezogenen Daten über einen Betroffenen öffentlich (gerade bei Internetveröffentlichungen) gemacht, ist der Verantwortliche künftig zusätzlich dazu verpflichtet, angemessene Maßnahmen zu treffen und andere verantwortliche Stellen darüber zu informieren, dass der Betroffene die Löschung aller Links zu diesen Daten sowie von Kopien verlangt. Zu beachte ist die generelle Löschpflicht, die besteht, ohne dass der Betroffene sein Recht explizit geltend macht.

Die Ausnahmen von der generellen Löschpflicht sind recht eng gefasst. Verantwortliche müssen personenbezogene Daten ggf. auch dann löschen, wenn die betroffene Person Widerspruch gegen die Verarbeitung (Art. 21) ihrer personenbezogenen Daten einlegt. Kann der Verantwortliche in diesem Fall nicht nachweisen, dass vorrangige berechtigte Gründe für die Verarbeitung vorliegen, muss er die in Frage stehenden Daten löschen.

Gesetzliche Aufbewahrungsfristen sind in allen genannten Fällen zu berücksichtigen und einzuhalten.

## 6. Personenbezogene Daten von Kindern

Erstmals wird ausdrücklich festgelegt, dass eine Einwilligung in die Datenverarbeitung personenbezogener Daten erst mit 16 Jahren möglich ist. Zuvor bedarf es der elterlichen Einwilligung. Dabei ist wichtig, dass eine nachträgliche Genehmigung ausdrücklich ausgeschlossen ist.

## 7. Datenschutzfolgenabschätzung (DSFA), Art. 35

Eine DSFA muss bei allen neuen oder bestehenden, stark veränderten Verfahren durchgeführt werden, wenn durch die Datenverarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen besteht. Unabhängig vom Risiko ordnet die DSGVO für besonders sensible Fälle die zwingende Durchführung der Folgenabschätzung an. Dies sind die automatische Verarbeitung von Daten, Profilbildungsmaßnahmen und die systematische Überwachung öffentlich zugänglicher Bereiche. Weitere Fälle werden durch die Aufsichtsbehörden in Form einer Blacklist (muss) und Whitelist (muss nicht) festgelegt. Bei neuen oder stark veränderten Verfahren (u.a. neue Technologien) ist die durchzuführende Prüfung, ob die Durchführung einer DSFA erforderlich ist, auch dann zu dokumentieren und nachzuweisen, wenn im Ergebnis die DSFA selbst nicht durchgeführt werden muss.

## 8. Prinzip des „One-Stop-Shop"

Das Prinzip des „One-Stop-Shop" (zu Deutsch das Prinzip der einheitlichen Anlaufstelle) besagt, dass künftig für grenzüberschreitende Datenvereinbarungen innerhalb der EU grundsätzlich die Aufsichtsbehörde am Sitz der Hauptniederlassung federführend zuständig sein wird. Diese ist dann auch alleiniger Ansprechpartner für die Verpflichteten.

## 9. Meldepflicht von „Datenpannen"

Die Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche, bspw. das Unternehmen, ohne schuldhaftes Zögern und möglichst binnen 72 Stunden nachdem die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde melden, sofern nicht ein Risiko für die Rechte und Freiheiten natürlicher Personen ausgeschlossen ist (Art. 33).

## 10. Erleichterte Datenübermittlung im Konzern

Die Weitergabe personenbezogener Daten zwischen Konzernunternehmen wird mit der DSGVO vereinfacht werden. Denn Erwägungsgrund 48 stellt erfreulich deutlich klar, dass Verantwortliche, die Teil einer Unternehmensgruppe sind, ein berechtigtes Interesse haben können, „personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln." Diese Klarstellung wird gerade den konzerninternen Austausch von Daten grundsätzlich erleichtern, auch wenn die Übermittlung an Empfänger außerhalb der EU weiterhin erheblichen Anforderungen unterliegt, vgl. Art. 44 ff. DSGVO.

## 11. Datenverarbeitung Beschäftigungsverhältnis, § 26

Die Verarbeitung für Zwecke des Beschäftigungsverhältnisses ist zulässig,

- wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder
- nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder
- zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Besonderheiten sind bei der

- Einwilligung (Berücksichtigung möglicher Abhängigkeit, Schriftform) und
- zur Aufdeckung von Straftaten

zu berücksichtigen.

Abweichend von Art. 9 Abs. 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Eine Zulässigkeit der Verarbeitung ist auch auf der Grundlage von Kollektivvereinbarungen herzustellen, aber zurzeit noch nicht erfolgt.

## 12. Haftung

Durch die DSGVO wird die Haftung erheblich verschärft. So wird bei Verstößen gegen die Grundprinzipien der DSGVO ein Bußgeld von bis zu 20 Mio. EUR oder bis zu vier Prozent des weltweiten letztjährigen Jahresumsatzes angedroht. Für leichtere Verstöße gegen Pflichten aus der DSGVO ist ein Bußgeld von maximal zehn Mio. EUR oder von zwei Prozent des weltweiten letztjährigen Jahresumsatzes vorgesehen.

# WEG ZUR EU-DATENSCHUTZ-GRUNDVERORDNUNG

## 1. Sensibilisierung

Geschäftsführungen, Datenschutzbeauftragte und andere für das Thema Datenschutz

Zuständige sollten innerhalb des Unternehmens dafür sensibilisieren, dass sich ab dem 25.

Mai 2018 nicht nur der Name der wichtigsten Datenschutzvorschriften ändern wird. Anders als eine EU-Richtlinie ist eine EU-Verordnung direkt in den Mitgliedstaaten der Europäischen Union anwendbar, also auch in Deutschland. Neben der DSGVO wird es weiterhin ein – neues – Bundesdatenschutzgesetz und sektorales Fachrecht mit ausführenden Regelungen zur DSGVO geben.

## 2. Risikoanalyse

Vor allem aufgrund der steigenden Bußgeld- und Reputationsverlustrisiken sowie künftig drohender Schadenersatzforderungen betroffener Personen ist eine auf das gesamte Unternehmen und die einzelnen Geschäftsbereiche bezogene Risikoanalyse empfehlenswert. Denkbare Risiken sind beispielsweise:

- Betroffenenrechte • Arbeitsrechtliche Aspekte • Mögliche Bußgelder • Umgang mit Aufsichtsbehörden • Zivilrechtliche Haftungsrisiken • Reputationsschäden

## 3. Bestandsaufnahme

Um Änderungsbedarf identifizieren zu können, sollte eine Bestandsaufnahme sämtlicher Prozesse und Verfahren durchgeführt werden, in denen personenbezogene Daten verarbeitet werden. Wegen des gegenüber dem aktuelle BDSG deutlich stärker risikobasierten Ansatzes der DSGVO kommen neben der Nutzung bereits bestehender Datenschutzstrukturen auch die Adaption von Prozessen und Strukturen eines bestehenden Compliancemanagements oder Qualitätsmanagementsystems in Betracht.

## 4. Gap-Analyse

Das Unternehmen sollte für die erfolgreiche Umsetzung der Vorgaben der DSGVO einen strukturierten Abgleich des Ist-Zustandes mit dem künftigen Soll-Zustand vornehmen. Auf dieser Grundlage lassen sich dann alle weiteren Schritte planen. Die Gap-Analyse ist ein wichtiger Baustein jeglicher Projektplanung zum Thema Datenschutz, insbesondere bei der Umsetzung vorgeschriebener Transparenz- und Dokumentationspflichten.

## 5. Einbindung des Datenschutzbeauftragten

Der betriebliche oder externe Datenschutzbeauftragte muss ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden. Außerdem sollte das Unternehmen die Umsetzung dieser Anforderung in einer dem Art. 24 entsprechenden Weise dokumentieren.

Der Datenschutzbeauftragte ist gleichzeitig verpflichtet, sein Unternehmen und die Beschäftigten in Datenschutzfragen zu beraten.

## 6. Datenschutzkommunikation

Viele Unternehmen werden dem Datenschutz aufgrund der Vorgaben der DSGVO in Zukunft einen höheren Stellenwert zumessen müssen als nach den bisherigen Vorgaben des BDSG. Dies setzt ein klares Bekenntnis der Unternehmensführung zum Datenschutz sowie eine entsprechende Kommunikation gegenüber der Belegschaft und den Kunden voraus.

Bei größeren Unternehmen bietet sich dazu – sofern nicht bereits vorhanden – die Einführung einer Datenschutzrichtlinie oder eine entsprechende Überarbeitung der EDV-Richtlinie an.

## 7. Mitarbeiterschulungen

Aufgrund der Komplexität und den vielfältigen Anforderungen der DSGVO sollten von den Änderungen betroffene Mitarbeiter gründlich im Umgang mit den Neuregelungen geschult werden. Der Datenschutzbeauftragte ist nach Art. 39 Abs. 1 lit. b der DS-GVO ausdrücklich zur „Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter" angehalten.

## 8. Betriebsrat und Betriebsvereinbarungen

Aus Unternehmersicht empfiehlt es sich zu Fragen der Umsetzung der DSGVO frühzeitig den Betriebsrat in die Umsetzungsprozesse mit einzubeziehen. Aufgrund der DSGVO können außerdem teilweise erhebliche Anpassungen bei bestehenden Betriebsvereinbarungen notwendig werden. Zudem kann auch der Abschluss neuer Betriebsvereinbarungen Sinn machen.

## 9. Rechtzeitige Planung neuer Prozesse und Strukturen

Nach der DSGVO werden zahlreiche neue Prozesse und Strukturen vorausgesetzt, die die Unternehmen bis Ende Mai 2018 umsetzen müssen. Dabei sollten insbesondere folgende Anforderungen besonders berücksichtigt werden:

**a) Datenschutzdokumentation**

Die DSGVO enthält zahlreiche Dokumentationspflichten, wie etwa das Führen eines

Verzeichnisses von Verarbeitungstätigkeiten (Art. 30, s. auch o. Teil II), die Dokumentation von Weisungen bei Auftragsverarbeitungsverhältnissen (Art. 28 Abs. 3) sowie die rechtzeitige Meldung von Datenschutzvorfällen (Art. 33 Abs.5).

**b) Privacy by design, privacy by default**

Unternehmen sind in Zukunft nach Art. 25 DSGVO dazu verpflichtet, die geltenden Datenschutzvorschriften durch eine datenschutzfreundliche Gestaltung der eingesetzten IT und entsprechende Voreinstellungen umzusetzen. Unternehmen müssen dies durch geeignete technische Maßnahmen umsetzen, etwa durch auf Datenminimierung ausgerichtete IT-Systeme und eine möglichst frühzeitige Pseudonymisierung von personenbezogenen Daten.

### c) Beschwerdemanagement zur Wahrung der Betroffenenrechte

Nach der DSGVO stehen den von einer Verarbeitung von personenbezogenen Daten betroffenen Personen verschiedenen Mechanismen zur Geltendmachung ihrer Rechte zur Verfügung. Dies äußert sich etwa in dem Auskunftsrecht nach Art. 15, das deutlich umfangreicher ist als das bisher nach § 34 BDSG bestehende.

Außerdem sieht die DSGVO u. a. ein Recht auf Berichtigung (Art. 16), das „Recht auf Vergessenwerden" (Art. 17), ein Recht auf Datenübertragbarkeit (Art. 20), das Recht auf Einschränkung der Verarbeitung (Art. 18) sowie ein Widerspruchsrecht (Art. 21) vor.

Die Umsetzung dieser Betroffenenrechte legt nahe, dass Unternehmen – zumindest Unternehmen entsprechender Größe - ein entsprechendes Beschwerde-management einrichten sollten, um die Geltendmachung der genannten Ansprüche umsetzen zu können, andernfalls droht Haftung.

### d) Vertragsmanagement

Unternehmen sollten ein Vertragsmanagement für Verträge mit datenschutzrechtlichem Bezug einführen und bis zur Geltung der DSGVO sicherstellen, dass bestehende Auftragsdatenverarbeitungsverträge (ADV), Verträge zur Übermittlung von personenbezogenen Daten und sonstige Verträge, die die Verarbeitung personenbezogener Daten beinhalten, den Anforderungen der Art. 28 und 29 entsprechen.

### e) Einwilligungsmanagement

Die DS-GVO stellt hohe Anforderungen an die Einwilligung betroffener Personen in die Verarbeitung ihrer personenbezogenen Daten. Daher sollte strukturiert geprüft und dokumentiert werden, an welchen Stellen personenbezogene Daten auf welcher Grundlage verarbeitet werden, um bestehende Prozesse von den bisherigen Vorgaben auf die des Art. 7 umzustellen. Nach dem Beschluss des Düsseldorfer Kreises vom 14.September 2016 gelten bisher erteilte Einwilligungen fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171). Bereits rechtswirksam erteilte Einwilligungen erfüllen grundsätzlich diese Bedingungen. Informationspflichten nach Art. 13 DS-GVO müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.