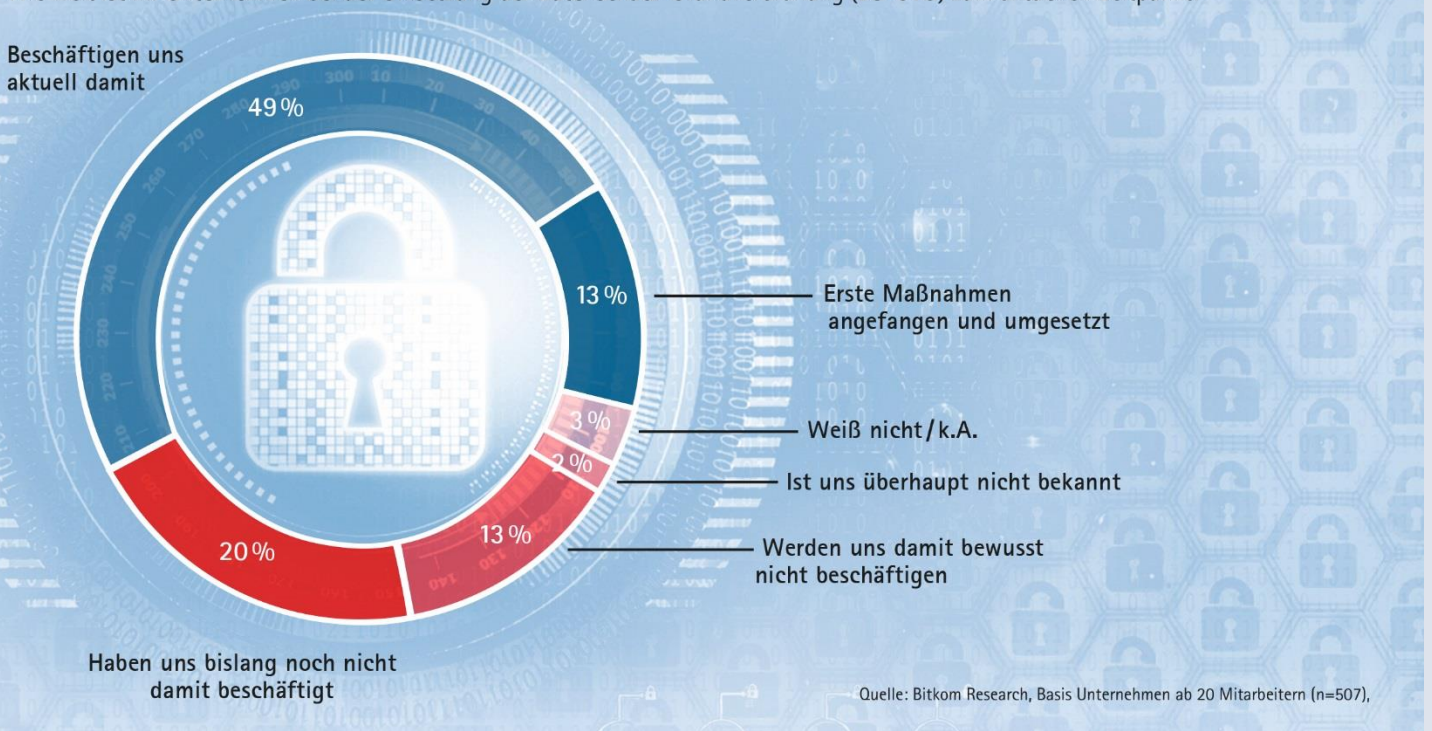


Die Datenschutz-Grundverordnung kommt! Dringender Handlungsbedarf bei den Unternehmen

Jedes dritte Unternehmen ignoriert bislang die DS-GVO

Wie weit ist Ihr Unternehmen bei der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) zum aktuellen Zeitpunkt?

Beschäftigen uns
aktuell damit



Haben uns bislang noch nicht
damit beschäftigt

Quelle: Bitkom Research, Basis Unternehmen ab 20 Mitarbeitern (n=507).

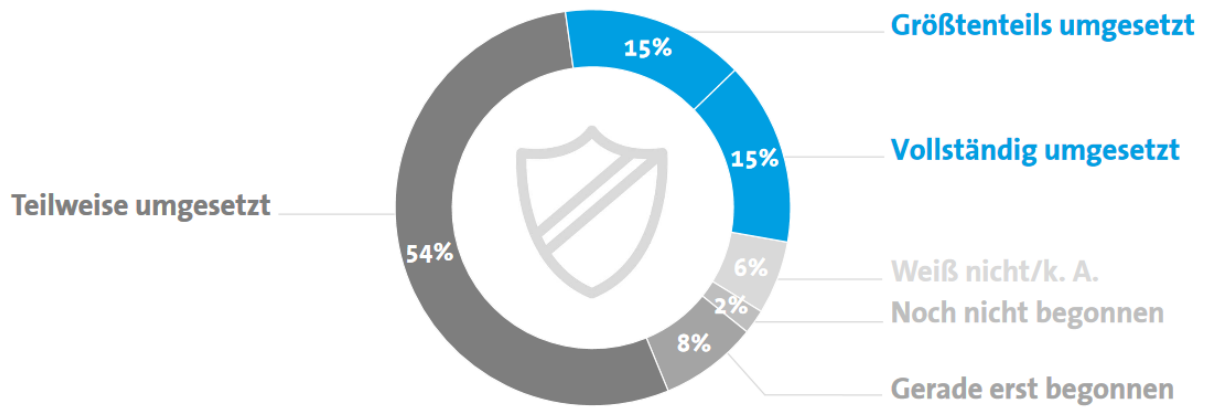
Am 25. Mai 2018 wird die Datenschutz-Grundverordnung (DS-GVO) für alle Unternehmen und Behörden verbindlich. Die neuen Regeln sind weitreichend. Bei Verstößen drohen drakonische Bußgelder von bis zu 20 Millionen Euro oder 4 % des globalen Jahresumsatzes. Dies gilt auch für kleine Unternehmen.

Gleichwohl hat sich jedes dritte Unternehmen gemäß einer repräsentativen Umfrage des IT-Branchenverbandes Bitkom noch nicht mit der Umsetzung der neuen Regelungen beschäftigt (siehe Grafik)!

Lesen Sie mehr zum Thema sowie Handlungsempfehlungen für Unternehmen auf den folgenden Seiten im aktuellen „Fokus Niedersachsen“ der IHK Niedersachsen (IHKN).

Große Mehrheit wird die DS-GVO nicht pünktlich umsetzen

Wie weit wird Ihr Unternehmen mit der Umsetzung der DS-GVO am 25. Mai 2018 sein?



8 Basis: Unternehmen, die sich bereits mit der DS-GVO auseinandergesetzt haben oder dies noch tun wollen (n=417) | Quelle: Bitkom Research

bitkom

Nach einer aktuellen Umfrage von Bitkom ist klar: Eine große Mehrheit der Unternehmen wird die DS-GVO nicht in allen Punkten pünktlich umsetzen können. Nur 30 % der befragten Unternehmen haben die Anforderungen bereits vollständig oder größtenteils

implementiert. Um Nachteile zu vermeiden, sollten jedoch auch die Unternehmen, die mit der Umsetzung noch gar nicht begonnen haben, jetzt schnellstens tätig werden.

Die DS-GVO gilt für alle EU-Mitgliedsstaaten unmittelbar und soll eigentlich für mehr Rechtssicherheit und faire Wettbewerbsbedingungen sorgen. Bisher gilt nämlich nur eine EU-Datenschutzrichtlinie, die von allen Mitgliedstaaten jeweils in nationales Recht umgesetzt wurde und damit einen Flickenteppich an unterschiedlichen Regelungen hervorgebracht hat. Insofern sind der beabsichtigte Zweck und die (vermeintliche) Vereinheitlichung grundsätzlich zu begrüßen. Doch bei näherer Betrachtung zeigen sich die Tücken: Die DS-GVO wimmelt nämlich nur so von Öffnungsklauseln. Diese ermöglichen es den Mitgliedstaaten viele Bereiche individuell auszugestalten – und dies wird genutzt. Man muss daher eigentlich von einem „Hybrid“ zwischen Richtlinie und Verordnung sprechen.

Das bisherige Bundesdatenschutzgesetz (BDSG – gilt für alle Unternehmen sowie für die Behörden des Bundes) und das Niedersächsische Datenschutzgesetz (NDSG – gilt für die niedersächsischen Landesbehörden) werden also nicht durch die DS-GVO gänzlich ersetzt, sondern regeln künftig nur noch die Bereiche, die nicht allein der Verordnung vorbehalten sind. Für Juristen und IT-Fachkräfte in Unternehmen und Behörden bedeutet dies doppelte Arbeit: Sie müssen zunächst in die DS-GVO und anschließend in das neue BDSG, bzw. neue NDSG schauen, bevor es an die rechtliche Bewertung bzw. technische Umsetzung geht. Keine einfache Aufgabe.

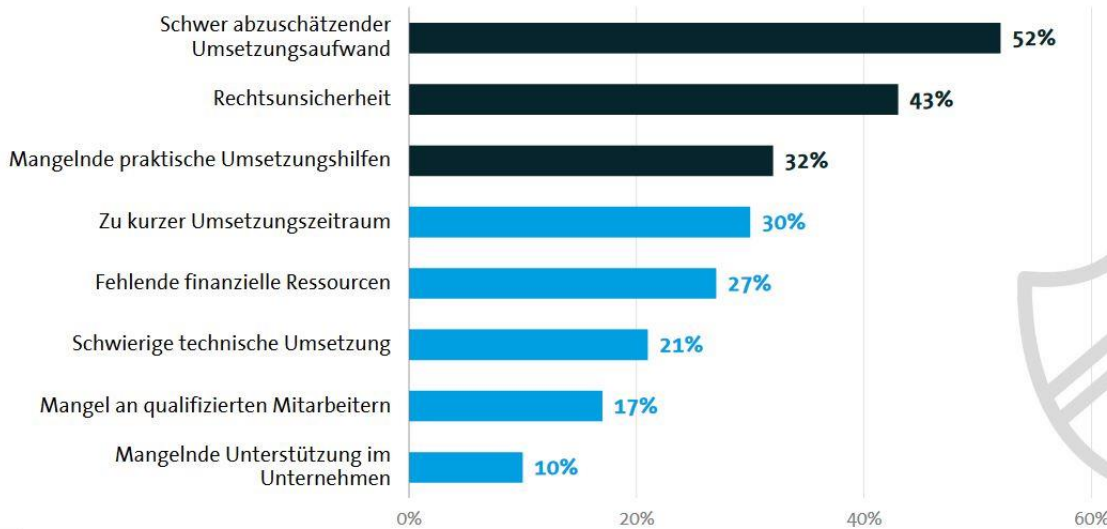
Schwer abzuschätzender Umsetzungsaufwand und Rechtsunsicherheit machen den Unternehmen schaffen

Viele Unternehmen können den Aufwand zur Umsetzung nur schwer abschätzen und sind unsicher, wie sich das neue Recht

auswirkt. Dies sind die beiden größten Herausforderungen für die niedersächsischen Unternehmen.

Unsicherheit macht den Unternehmen zu schaffen

Welches sind die größten Herausforderungen bei der Umsetzung der DS-GVO?



bitkom

Basis: Unternehmen, die sich bereits mit der DS-GVO auseinandergesetzt haben oder dies noch tun wollen (n=417) | Mehrfachnennungen möglich |
 9 Quelle: Bitkom Research

Die sieben Industrie- und Handelskammern in Niedersachsen bieten ihren Mitgliedsunternehmen bereits seit längerer Zeit umfangreiche Informationen zum Thema an – in Online-Publikationen, Newslettern, Pressemeldungen, Veranstaltungen und/oder durch Beiträge in den IHK-Magazinen. Darüber hinaus begleitet die IHK Niedersachsen (IHKN) das Gesetzgebungsverfahren in Nieder-

sachsen kritisch zum Wohle der niedersächsischen Wirtschaft.

In jeder IHK gibt es einen Ansprechpartner für Fragen zur DS-GVO. Die Kontaktdaten finden Sie auf Seite 7.

Die neun Säulen der DS-GVO

Um den Schutzgedanken der neuen DS-GVO zu verstehen, macht es Sinn, sich zunächst die „Neun Säulen“ des Datenschutzes zu

vergegenwärtigen. Sie bilden die Grundlage der DS-GVO.



Mit der DS-GVO werden zahlreiche bereits bestehende Regelungen modifiziert und ergänzt. Unternehmen sollten sich angesichts -

der Tragweite der neuen Regelungen frühzeitig mit den Änderungen vertraut machen – die Zeit drängt!

Die wichtigsten Änderungen im Überblick:

- ✓ Verschärfte Rechenschafts- und Dokumentationspflichten.
- ✓ Erweiterung der Betroffenenrechte im Hinblick auf Einwilligung, Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung.
- ✓ Verschärfte Meldepflichten bei Datenpannen.
- ✓ „Privacy by design“ und „Privacy by default“: Hard- und Software müssen so konzipiert und voreingestellt sein, dass sie möglichst nur die Daten erfassen können, die zur Erfüllung des rechtmäßigen Zwecks unbedingt erforderlich sind (Prinzip der Datenminimierung).
- ✓ Drastische Erhöhung der Bußgelder bei Verstoß, „20/4“: Bisher sah das BDSG einen Rahmen bis zu 300.000 Euro pro Verstoß vor. Künftig gilt bei Verstößen durch natürliche Personen ein Rahmen von bis zu 20 Millionen Euro. Unternehmen als Körperschaften müssen mit einem Satz von bis zu 4 % ihres globalen Umsatzes rechnen. Bei größeren Unternehmen oder Konzernen können so schnell dreistellige Millionenbeträge entstehen.
- ✓ Erhöhte Verantwortung der Datenschutzbeauftragten: Sie haben künftig nicht nur überwachende und beratende Funktion, sondern es gilt ein ganzer Kanon an konkret definierten gesetzlichen Aufgaben.
- ✓ Verschärfte Anforderungen bei Datentransfer in Drittstaaten: Dies ist bereits bei der Verwendung von „Clouds“ außerhalb der EU der Fall.
- ✓ Zusätzliches Verfahrensverzeichnis für die sogenannte „Auftragsdatenverarbeitung“ – ein in der Praxis sehr häufig vorkommender Vorgang.
- ✓ Erleichterter Datenaustausch im Konzern.

 **Besonders wichtige Aspekte für Unternehmen**

I. Datenschutzbeauftragter

Jedes Unternehmen muss einen Datenschutzbeauftragten ernennen, wenn es mehr als neun Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt. Dabei reicht es schon, wenn mehr als neun PC-Arbeitsplätze zur Verfügung stehen. In Branchen, die mit besonders sensiblen Daten zu tun haben, wie zum Beispiel dem Gesundheitswesen, besteht diese Pflicht auch unabhängig von der Mitarbeiteranzahl. Eine freiwillige Bestellung eines Datenschutzbeauftragten ist möglich und oftmals angesichts der Komplexität der Materie auch zu empfehlen.

Zu den Aufgaben des Datenschutzbeauftragten gehören im Wesentlichen die Unterrichtung und Beratung der verantwortlichen Geschäftsführung in datenschutzrechtlichen Fragen, die Überwachung und Einhaltung der datenschutzrechtlichen Vorschriften, Sensibilisierung und Schulung von Mitarbeitern, Beratung bei der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung. Darüber hinaus ist er wichtiger Vermittler zwischen den Beteiligten, wie zum Beispiel Aufsichtsbehörden, Betroffenen und den für die Datenverarbeitung Verantwortlichen. Der Datenschutzbeauftragte ist weisungsunabhängig bei seiner Aufgabenerfüllung und berichtet unmittelbar der höchsten Managementebene. Die

Verantwortlichkeit für die Einhaltung des Datenschutzes verbleibt allerdings bei der Geschäftsführung.

Die Unternehmensleitung kann entweder einen eigenen Mitarbeiter oder einen externen Dienstleister zum Datenschutzbeauftragten ernennen. Dieser darf wegen der Erfüllung seiner Aufgaben weder abberufen noch benachteiligt werden. Sofern ein Mitarbeiter zum Datenschutzbeauftragten ernannt wird, genießt er im Rahmen des BDSG besonderen Kündigungsschutz.

Neu ist, dass eine Unternehmensgruppe (zum Beispiel ein Konzern) einen gemeinsamen Datenschutzbeauftragten ernennen kann. Voraussetzung hierfür ist, dass der Datenschutzbeauftragte von jeder Niederlassung aus leicht erreicht werden kann.

Grundsätzlich bleibt übrigens eine jetzt schon vorhandene Ernennung auch nach dem 25. Mai 2018 weiterhin gültig.

II. Dokumentationspflichten und Verarbeitungsverzeichnis

Die DS-GVO legt an verschiedenen Stellen Dokumentationspflichten fest, die deutlich von den bisherigen Regelungen abweichen. Unternehmen müssen zukünftig nachweisen können, dass ihre Datenverarbeitung den datenschutzrechtlichen Anforderungen entspricht. Diese Nachweispflicht erfordert eine umfassende Dokumentation. Beispielhaft für die Dokumentationspflichten der DS-GVO kann das Verzeichnis von Verarbeitungstätigkeiten genannt werden. Dieses Verarbeitungsverzeichnis dient dem Nachweis, dass die DS-GVO eingehalten wird und ist daher von zentraler Bedeutung. Der Umfang der Dokumentation umfasst grundsätzlich alle Verfahren des Unternehmens, bei denen personenbezogene Daten verarbeitet werden.

Die Dokumentation von Datenschutzvorfällen ist darüber hinaus zukünftig verpflichtend. Jede Datenverletzung muss der zuständigen Datenschutzaufsichtsbehörde innerhalb von 72 Stunden gemeldet und dokumentiert werden. Dabei müssen alle Fakten, Auswirkungen und ergriffene Abhilfemaßnahmen festgehalten werden. Für Unternehmen ist es deshalb zukünftig wichtig, eine umfassende und lückenlose Dokumentation zu führen und im Falle einer Prüfung, die oftmals unangekündigt erfolgt, vorweisen zu können.

III. Arbeitnehmerdaten

In der DS-GVO gibt es keine detaillierten inhaltlichen Regelungen zum Beschäftigtendatenschutz. Vielmehr enthält sie eine Öffnungsklausel, wonach die Mitgliedsstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften hinsichtlich der Datenverarbeitung im Beschäftigungskontext vorsehen können. Der deutsche Gesetzgeber hat von dieser Möglichkeit im neuen BDSG Gebrauch gemacht. Es wird

ebenfalls am 25. Mai 2018 in Kraft treten und orientiert sich beim Beschäftigtenschutz an den bisherigen Regelungen: Die Verarbeitung von personenbezogenen Daten bleibt zulässig, soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung oder dies zur Erfüllung gesetzlicher Pflichten erforderlich ist.

Zukünftig können Tarifverträge, Betriebs- oder Dienstvereinbarungen (Kollektivvereinbarungen) geeignete Rechtsgrundlagen für eine mögliche Datenverarbeitung schaffen. Werden für die Datenverarbeitung Einwilligungen der Mitarbeiter eingeholt, beispielsweise zur Verwendung eines Fotos des Mitarbeiters im Internet, müssen die Mitarbeiter auf das jederzeitige Widerrufsrecht hingewiesen werden. Die bisherigen Einwilligungen der Mitarbeiter soll-

ten nun auf Konformität mit der DS-GVO überprüft werden.

Insgesamt sehen die neuen Regelungen der DS-GVO und des BDSG mehr Informationspflichten der Arbeitgeber und mehr Auskunftsrechte der Mitarbeiter über die gespeicherten Daten vor.

IV. Videoüberwachung

Viele Unternehmen nutzen moderne Videoüberwachungsanlagen, um ihre Betriebsgrundstücke und -anlagen zu überwachen, um Straftaten im Unternehmen aufzuklären und um ihr Hausrecht auszuüben. Für solche Überwachungsmaßnahmen gibt es auch bisher rechtliche Regeln, die über deren Zulässigkeit entscheiden. So sieht bereits das jetzige BDSG vor, dass die Kameraüberwachung öffentlich zugänglicher Räume (wie Verkaufsräume, Schalterhallen, Parkplätze) zur Wahrnehmung des Hausrechts oder zum Schutz der Kunden und Mitarbeiter erlaubt ist. Die Überwachung öffentlich zugänglicher großflächiger Anlagen wie beispielsweise Sport- und Vergnügungsstätten oder Einkaufszentren zum Schutz der Besucher ist sogar unter erleichterten Bedingungen möglich. Auch in Bereichen eines Betriebes, die nicht für die Öffentlichkeit zugänglich sind, ist die Überwachung durch Kameras insbesondere dann erlaubt, wenn ein konkreter Verdacht besteht, dass Mitarbeiter Straftaten gegen das Unternehmen begehen und eine Aufklärung anderweitig nicht möglich ist. Im Gegensatz zum BDSG enthält die DS-GVO kaum konkrete Regelungen zur Zulässigkeit der Videoüberwachung. Erwähnt wird sie lediglich in Artikel 35 DS-GVO, der die Notwendigkeit einer sogenannten „Datenschutz-Folgenabschätzung“ vorsieht, sofern eine „systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche“ stattfindet.

Umfang dieser Datenverarbeitung sowie über ihre potentiellen Risiken für das Persönlichkeitsrecht der Betroffenen machen und seine Erwägungen schriftlich niederlegen. Dabei bleibt es auch im neuen Recht, wobei die Gerichte noch werden klären müssen, was genau eine „systematische umfassende“ Überwachung ist. Je nachdem, wie streng diese Auslegung am Ende ausfällt, könnte es dabei durchaus auch zu bürokratischer Entlastung der Unternehmen kommen, wenn die zeitraubende Folgenabschätzung im Einzelfall entfällt. Aufwändiger wird es dagegen künftig, wenn eine Person anhand eines Überwachungsvideos tatsächlich identifiziert wird. In diesem Fall muss sie zwar auch schon bisher über bestimmte Tatsachen wie die Identität des Betreibers der Überwachungsanlage und den Zweck der Beobachtung informiert werden. Die Menge der Informationen, die zur Erfüllung dieser Pflicht mitzuteilen sind, wird sich aber durch die DS-GVO nicht unerheblich erweitern. So muss künftig auch darüber informiert werden, ob die Daten an einen Empfänger in einem Drittland außerhalb der EU übermittelt werden, wie lange die Videos gespeichert werden, welche Rechte auf Löschung oder Sperrung der Daten bestehen und noch einiges mehr. Im Ergebnis bringt die DS-GVO auf dem Feld der Videoüberwachung primär formale Neuerungen, während die inhaltlichen Kriterien der Zulässigkeit solcher Kontrollmaßnahmen sich gegenüber der derzeitigen Rechtslage kaum ändern werden.

Wer eine Videoüberwachung einrichtet, sollte sich also im Vorfeld intensiv Gedanken über den konkreten Zweck und notwendigen

V. Technische und organisatorische Maßnahmen („TOMs“)

Die Anforderungen der DS-GVO an die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten bauen weitestgehend auf den bereits geltenden Regelungen auf. Verantwortliche haben demnach geeignete technische und organisatorische Maßnahmen zu treffen, um unter Berücksichtigung des Stands der Technik und der Schwere des Risikos ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten. Als technische Maßnahmen sind physische Schutzvorkehrungen wie die Sicherung von Türen oder IT-be-

zogene Schutzvorkehrungen wie die Passwörterzwangung oder die Pseudonymisierung von Daten zu verstehen. Unter organisatorischen Maßnahmen werden prozessuale Vorkehrungen wie das Vier-Augen-Prinzip oder etwa die Pflicht zur Anmeldung von Besuchern verstanden. Technische und organisatorische Maßnahmen müssen dem aktuellen Stand entsprechen und daher regelmäßig überprüft und angepasst werden.

Übergeordnete Sicherheitsziele der DS-GVO sind die dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste. Das angemessene Schutzniveau für sämtliche Datenverarbeitungsprozesse im Unternehmen muss durch die für die Datenverarbeitung verantwortliche Stelle sichergestellt werden. Dies gilt auch bei Auslagerung des Betriebs technischer Systeme an externe Dienstleister. Über die bisherigen Regelungen hinausgehend müssen bei der Planung und Umsetzung technisch-organisatorischer Maßnahmen

zukünftig auch die Implementierungskosten und das von dem Datenverarbeitungsverfahren ausgehende Risiko zur Beeinträchtigung von Persönlichkeitsrechten berücksichtigt werden. Das anzustrebende Schutzniveau und die Implementierungskosten sollen somit in einem angemessenen Verhältnis zueinander stehen. Mittels einer vor Inbetriebnahme durchzuführenden Datenschutz-Folgenabschätzung ist dafür das sich aus einem Datenverarbeitungsverfahren ergebende Risiko zu ermitteln.

In der Anlage stellen wir Ihnen ergänzend einen 10-Punkte-Plan der Aufsichtsbehörden zur Verfügung.

► Ansprechpartner für den Fokus Niedersachsen

IHKN-Sprecher für Recht

Bernd Seifert, Tel. 0441 2220 360, E-Mail: bernd.seifert@oldenburg.ihk.de

Ansprechpartner für Fragen zur DS-GVO in den einzelnen Kammern:

IHK Braunschweig: Johannes Sauter, Tel.: 0531 / 4715 225, E-Mail: johannes.sauter@braunschweig.ihk.de

IHK Hannover: Marc Weigand, Tel.: 0511 / 3107 338, E-Mail: weigand@hannover.ihk.de

IHK Lüneburg-Wolfsburg: Herbert Blank, 04131 / 742 172, E-Mail: blank@lueneburg.ihk.de

Oldenburgische IHK: Claudia Poneleit, Tel.: 0441 / 2220 362, E-Mail: claudia.poneleit@oldenburg.ihk.de

IHK Osnabrück - Emsland - Grafschaft Bentheim: Katrin Schweer, Tel.: 0541 / 353 325,

E-Mail: schweer@osnabrueck.ihk.de

IHK für Ostfriesland und Papenburg: Simon Alex, Tel. 04921 / 8901 83, E-Mail: simon.alex@emden.ihk.de

IHK Stade für den Elbe-Weser-Raum: Eike Thiel, Tel.: 04141 / 524 152, E-Mail: eike.thiel@stade.ihk.de

IHK Niedersachsen (IHKN)

Schiffgraben 57, 30175 Hannover

Tel. 0511 920 901 10

E-Mail: info@ihk-n.de

Die IHK Niedersachsen ist die Landesarbeitsgemeinschaft der IHK Braunschweig, IHK Hannover, IHK Lüneburg-Wolfsburg, Oldenburgischen IHK, IHK Osnabrück - Emsland - Grafschaft Bentheim, IHK für Ostfriesland und Papenburg sowie IHK Stade für den Elbe-Weser-Raum. Sie vertritt rund 460.000 gewerbliche Unternehmen gegenüber Politik und Verwaltung.

Der Fokus Niedersachsen erscheint in regelmäßigen Abständen zu aktuellen Themen aus Wirtschaft und Politik und steht unter www.ihk-n.de/Publikationen auch zum Download zur Verfügung.

Bitte beachten:

Zur besseren Lesbarkeit wird in dieser Publikation auf die geschlechtsneutrale Differenzierung verzichtet. Sämtliche Personenbezeichnungen gelten im Sinne der Gleichbehandlung für alle Geschlechter.

10-Punkte-Plan der Aufsichtsbehörden

Auf dem Weg zur EU Datenschutz-Grundverordnung – Anregungen für Unternehmen

Die europäische Datenschutz-Grundverordnung (DS-GVO) bringt eine Reihe von Veränderungen in den datenschutzrechtlichen Anforderungen für den Umgang mit personenbezogenen Daten mit sich. Auch Auftrags(daten)verarbeiter müssen sich auf geänderte Rahmenbedingungen einstellen. Wir haben in 10 Punkten Anregungen für Unternehmen zusammengestellt.

1. Sensibilisierung durchführen

Geschäftsführungen, Datenschutzbeauftragte und andere für das Thema Datenschutz Zuständige sollten innerhalb des Unternehmens dafür sensibilisieren, dass sich ab dem 25.05.2018 nicht nur der Name einer europäischen Datenschutzregelung ändern wird. Die DS-GVO wird direkte Auswirkungen auf Unternehmen als datenverarbeitende Stellen haben. Anders als eine EU-Richtlinie ist eine EU-Verordnung direkt in den Mitgliedstaaten der Europäischen Union anwendbar, also auch in Deutschland. Neben der DS-GVO wird es weiterhin ein – neues – Bundesdatenschutzgesetz und sektorales Fachrecht mit ausführenden Regelungen zur DS-GVO geben. Bitte beachten Sie: bis zum 24.05.2018 (einschließlich) gilt das JETZIGE Bundesdatenschutzgesetz!

2. Bestandsaufnahme machen

Um Änderungsbedarf identifizieren zu können, sollte in einem ersten Schritt eine Bestandsaufnahme der Prozesse durchgeführt werden, in denen personenbezogene Daten verarbeitet werden. Das Verzeichnisse nach § 4d Bundesdatenschutzgesetz (BDSG) ist ein Ausgangspunkt zur Identifizierung von Verarbeitungsverfahren. Im Folgenden haben wir beispielhaft einige Themen zusammengestellt, bei denen sich für Unternehmen Änderungsbedarf ergeben kann.

3. Rechtsgrundlage prüfen

Auch unter der DS-GVO ist für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich (Artikel 6 bis 11 DS-GVO). Es ist zu prüfen, ob das neue Recht für alle Prozesse Rechtsgrundlagen bereitstellt.

4. Personenbezogene Daten von Kindern besonders prüfen

Besondere Anforderungen bestehen für den Umgang mit personenbezogenen Daten von Kindern, wenn es um die Einwilligung in Bezug auf Dienste der Informationsgesellschaft geht (Artikel 8 DS-GVO).

5. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy-by-Design“ und „Privacy-by-Default“) umsetzen

Die DS-GVO enthält bestimmte Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei Voreinstellungen umzusetzen sind (Artikel 25 DS-GVO).

6. Verträge checken

Unternehmen sollten insbesondere ihre bestehenden Verträge zur Auftrags(daten)verarbeitung überprüfen und überarbeiten. In den Artikeln 26 bis 28 DS-GVO sind Vorgaben für Vereinbarungen mit Auftrags(daten)verarbeitern und zwischen gemeinsam für die Verarbeitung Verantwortlichen geregelt.

7. Datenschutzfolgeabschätzung implementieren

Der europäische Gesetzgeber hat die bisherige Vorabkontrolle (§ 4d Abs. 5 BDSG) nicht in die DS-GVO übernommen. Sie wird abgelöst durch die Datenschutz-Folgeabschätzung (Artikel 35 DS-GVO). An eine Datenschutz-Folgeabschätzung kann sich eine verpflichtende Konsultation der zuständigen Aufsichtsbehörde anschließen (Artikel 36 DS-GVO).

8. Melde- und Konsultationspflichten organisieren

Die Melde- und Konsultationspflichten gegenüber den Aufsichtsbehörden (Artikel 33, 36 und 37 DS-GVO) müssen in den internen Abläufen des Unternehmens abgebildet werden.

9. Betroffenenrechte und Informationspflichten umsetzen

Die in der DS-GVO geregelten Betroffenenrechte müssen in den unternehmensinternen Abläufen abgebildet und gegenüber den Betroffenen umgesetzt werden, etwa das Recht auf Löschung (Artikel 17) und das Recht auf Datenübertragbarkeit (Artikel 20) einschließlich der übergreifenden Rahmenbedingungen (Artikel 12) sowie die Informationspflichten des Verantwortlichen (Artikel 13, 14).

10. Dokumentation organisieren

Die DS-GVO enthält an verschiedenen Stellen Dokumentationspflichten, beispielsweise in Artikel 30 (Verarbeitungsverzeichnis), Artikel 33 Abs. 5 (Dokumentation von Datenschutzvorfällen) oder Artikel 28 Abs. 3 lit. a (Dokumentation von Weisungen im Rahmen von Auftragsverarbeitungsverhältnissen).

Quelle: Die Landesbeauftragte für den Datenschutz Niedersachsen