TÜV SÜD Akademie

Mehr Sicherheit.
Mehr Wert.

Die neue EU-Datenschutz-Grundverordnung

Aus BDSG wird DSGVO

White Paper

Einleitung

Durch den technischen Fortschritt, die wachsende Globalisierung und die daraus resultierenden internationalen Verflechtungen in Europa ist es sinnvoll und notwendig, das Datenschutzrecht in Europa zu harmonisieren. Diese Harmonisierung wird mit der Datenschutz-Grundverordnung, kurz „EU-DSGVO“ geschaffen, die ab 2018 für alle Unternehmen in Deutschland Gültigkeit haben wird.

Ab dem 25.05.2018 wird die EU-DSGVO das direkt in allen Mitgliedstaaten der Europäischen Union anwendbare Recht und ersetzt damit in den grundlegenden Bereichen das bislang bestehende nationale Datenschutzrecht (z. B. das Bundesdatenschutzgesetz „BDSG“). Allerdings beinhaltet die EU-DSGVO an einigen Stellen so genannte Öffnungsklauseln, aufgrund derer die Mitgliedstaaten die EU-DSGVO durch weitere nationale Regelungsinhalte ergänzen können.

Die Zeit bis dahin scheint lang. Betroffene Unternehmen sollten diese Zeit dennoch gut nutzen, um sich auf die bevorstehenden Änderungen rechtzeitig vorzubereiten.

Der TÜV SÜD stellt im Rahmen dieses White Papers die wichtigsten allgemeinen Informationen zur EU-DSGVO vor.

TÜV SÜD Akademie GmbH

TÜV®

AC110-EUDSGVOWP-kb-210x297-w-16-05-31

Inhalt

1. Die wichtigsten Grundsätze und Regelungen 3
1.1 Transparenz- und Informationspflichten, Art. 12f. 3
1.2 Rechtmäßigkeit der Verarbeitung, Art. 5f. 3
1.3 Einwilligung eines Kindes, Art. 8 4
1.4 Profiling, Art. 22 4
1.5 Werbliche Ansprache und Direktmarketing, Art. 6 Absatz 1f. 4
1.6 Weiterverarbeitung, Art. 6 4
1.7 Recht auf Löschung („Vergessenwerden"), Art. 17 5
1.8 Recht auf Datenübertragbarkeit, Art. 20 5
1.9 Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24 5
1.10 Datenschutzfreundliche Voreinstellungen, Art. 25 6
1.11 Auftragsverarbeitung, Art. 28 und gemeinsame Verantwortliche, Art. 26 6
1.12 Benachrichtigungspflichten bei Datenschutzverletzungen, Art. 33 7
1.13 Sicherheit der Verarbeitung, Art. 32 7
1.14 Datenschutz-Folgenabschätzung, Art. 35 7
1.15 Aufgaben und Pflichten des Datenschutzbeauftragten, Art. 37ff. 8
1.16 Zertifizierungen, Art. 42 8
1.17 Internationale Datenübermittlung, Art. 44ff. 9
1.18 Haftung und Recht auf Schadensersatz, Art. 82 9
1.19 Haftungserstreckung auf ausländische Unternehmen, Art. 3 9
1.20 Bußgelder und Sanktionen, Art. 83ff. 10

2. Zusammenfassung und Ausblick 11

1. Die wichtigsten Grundsätze und Regelungen

1.1 Transparenz- und Informationspflichten, Art. 12f.

Durch die EU-DSGVO steigen die Informationspflichten, wenn personenbezogene Daten beim Betroffenen erhoben werden. Zu den bekannten Informationspflichten wie Identität der verantwortlichen Stelle, Zweckbestimmung und Kategorien von Empfänger, kommen nun zusätzlich Informationen wie

- Kontaktdaten des Verantwortlichen samt Stellvertretung
- Kontaktdaten des Datenschutzbeauftragten
- Berechtigte Interessen des Verantwortlichen
- Übermittlungsabsicht an ein Drittland oder eine internationale Organisation (und die damit verbundene Angemessenheitsentscheidung der Kommission)
- Dauer der Speicherung
- Rechte des Betroffenen wie Auskunft, Löschung, Berichtigung, Einschränkung und Widerrufsrecht, Beschwerderecht bei einer Aufsichtsbehörde, Erforderlichkeit der Bereitstellung der Daten
- Beim Profiling aussagekräftige Informationen über die Logik und Tragweite der angestrebten Auswirkungen.

TÜV SÜD-Praxishinweis

Implementieren Sie Prozesse, die sicherstellen, dass alle Pflichtangaben dem Betroffenen mitgeteilt und aktuell gehalten werden. Überarbeiten Sie Ihre Datenschutzerklärungen!

1.2 Rechtmäßigkeit der Verarbeitung, Art. 5f.

Grundsätzlich ändert sich an den bisherigen Voraussetzungen für die Verarbeitung von personenbezogenen Daten nichts. Nach wie vor ist eine Verarbeitung personenbezogener Daten u. a. nur rechtmäßig, wenn eine Einwilligung für einen oder mehrere Zwecke vorliegt, die Verarbeitung aufgrund eines Vertrages (oder vorvertragliche Maßnahmen) erforderlich ist, eine gesetzliche Grundlage vorliegt oder ein berechtigtes Interesse der verantwortlichen Stelle oder eines Dritten die Verarbeitung der personenbezogenen Daten erforderlich macht. Eine Datenverarbeitung kann dabei nicht auf eine gesetzliche Grundlage eines Drittstaates gestützt werden.

Die hohen Voraussetzungen, die bislang für die Einwilligung galten (Freiwilligkeit, verständliche Form, einfache Sprache), sind nach wie vor zu beachten. Die Schriftform wird nicht explizit gefordert, jedoch kann aus dem Umkehrschluss, dass eine Dokumentation der Einwilligung vorgehalten werden muss, darauf geschlossen werden, dass eine schriftliche Einwilligung empfehlenswert ist.
Wie auch in der Vergangenheit wird der Betroffene ein Recht auf Widerruf seiner Einwilligung für die Zukunft haben. Dieser muss so einfach wie die Erteilung der Einwilligung möglich sein – ein Widerruf auf „demselben“ Weg wie die Einwilligung ist grundsätzlich hierzu nicht herauszulesen. Das bislang geltende „Koppelungsverbot“ gilt auch nach der EU-DSGVO; der Vertragsschluss oder die Erbringung einer Dienstleistung darf also nicht von der Einwilligung des Betroffenen abhängig gemacht werden, wenn die Datenverarbeitung, für die der Betroffene seine Einwilligung erteilen soll, nicht für die Erfüllung des Vertrages erforderlich ist.

Sonderregelungen gibt es für die Einwilligung eines Kindes (siehe Abschnitt 1.3). Die Verarbeitung von sensiblen Daten ist grundsätzlich untersagt, außer es liegt eine Einwilligung des Betroffenen vor.

TÜV SÜD-Praxishinweis

Stellen Sie technisch und organisatorisch sicher, dass die Dokumentation der Einwilligung vorgehalten werden kann.

1.3 Einwilligung eines Kindes, Art. 8

Neu ist die Aufnahme der Einwilligungsvoraussetzungen eines Kindes. Diese ist nach der EU-DSGVO nur dann rechtmäßig, wenn das Kind das 16. Lebensjahr vollendet hat oder die Zustimmung der Eltern für die Datenverarbeitung erteilt wird.

TÜV SÜD-Praxishinweis

Entwickeln Sie technische und organisatorische Möglichkeiten, um die Zustimmung der Eltern nachweisen zu können.

1.4 Profiling, Art. 22

Die EU-DSGVO führt den Begriff des „Profilings" ein. Unter „Profiling" versteht man jede Art der automatisierten Verarbeitung personenbezogener Daten, die darauf abzielt, dass die Daten verwendet werden, um bestimmte persönliche Aspekte eines Betroffenen zu bewerten, zu analysieren oder vorherzusagen.

Durch die EU-DSGVO erhält jeder Betroffene das Recht, nicht ausschließlich einer solchen (auf einer automatisierten Verarbeitung beruhenden) Entscheidung unterworfen zu werden, wenn diese rechtliche Wirkungen entfalten oder den Betroffenen in einer ähnlicher Weise erheblich beinträchtigen kann. Dashalb sind verantwortliche Stellen zukünftig verpflichtet, geeignete Maßnahmen zu treffen, um die Rechte und Freiheiten sowie die berechtigten Interessen der Betroffenen zu wahren. Die Mindestforderung beinhaltet das Recht auf Eingreifen einer Person, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung.

TÜV SÜD-Praxishinweis

Sie sollten bestehende automatisierte Verarbeitungsprozesse auf deren zukünftige Rechtmäßigkeit hin überprüfen und Vorkehrungen treffen, um die genannten, essentiellen Betroffenenrechte gesetzeskonform zu gewährleisten.

1.5 Werbliche Ansprache und Direktmarketing, Art. 6 Absatz 1f.

Ganz neue Möglichkeiten zeichnen sich in Sachen Werbung bzw. Direktmarketing ab. Legen wir die heute gültigen Regelungen zu Grunde, so richtet sich beinahe jede Form des Direktmarketings nach dem Listenprivileg oder dem Erfordernis der rechtswirksamen Einwilligung. Neben diesen Grundregelungen gibt es heute bezüglich Telefon- und E-Mail-Werbung zahlreiche Sondernormen. Zudem existieren gesetzliche Spezialregelungen, die von der Einstufung des werbetreibenden Unternehmens selbst abhängen.

Die EU-DSGVO sieht zukünftig eine allgemeine Interessensabwägung zwischen den berechtigten Interessen des Unternehmens und den Interessen bzw. Grundrechten des Betroffenen (Beworbenen) vor. Ausweislich der Erwägungsgründe der EU-DSGVO ist die Verarbeitung personenbezogener Daten zum Zwecke des Direktmarketings zukünftig als ein berechtigtes Interesse eines Unternehmens zu betrachten.

TÜV SÜD-Praxishinweis

Sie sollten Ihre gesamten werblichen Aktivitäten überprüfen und die bestehenden eigenen wie auch bezogenen Werbepotenziale neu bewerten. Dabei sollten die bestehenden Werbestrategien datenschutzrechtlich neu durchdacht und aufgestellt werden.

1.6 Weiterverarbeitung, Art. 6

Der Grundsatz der Zweckbindung hat auch in der EU-DSGVO Einzug gefunden. Die Verordnung unterscheidet zwischen einer Erstverarbeitung und einer Weiterverarbeitung. Eine Weiterverarbeitung ist demnach nur dann zulässig, wenn sie mit dem ursprünglich festgelegten, eindeutigen und rechtmäßigen Zweck, weshalb die Daten erhoben worden sind, vereinbar ist. Dies wird als „Kompatibilitätsprüfung" bezeichnet, da festgestellt werden muss, ob der ursprüngliche Zweck der Erstverarbeitung auch mit dem Zweck der Weiterverarbeitung kompatibel ist.

TÜV SÜD-Praxishinweis

Sie sollten sicherstellen, dass sowohl bei Ersterhebung als auch bei Weiterverarbeitung ein eindeutig festgelegter und rechtmäßiger Zweck vorliegt.

1.7 Recht auf Löschung („Vergessenwerden"), Art. 17

Auch mit Geltung der EU-DSGVO ändert sich nichts an der gesetzlichen Vorgabe, dass personenbezogene Daten auch weiterhin im Fall des Zweckwegfalls zu löschen sind, wenn keine anderweitige Rechtsgrundlage eine weiterführende Verarbeitung rechtfertigen kann.

Neu hingegen ist eine speziell geregelte Löschverpflichtung für personenbezogene Daten von Kindern (bis zur Vollendung des 16. Lebensjahres). Des Weiteren müssen Unternehmen zukünftig einer neuen Handlungsverpflichtung in den Fällen nachkommen, in denen sie personenbezogene Daten „öffentlich" gemacht haben. Unter Berücksichtigung der verfügbaren Technologien und der Implementierungskosten angemessener Maßnahmen müssen Unternehmen zukünftig andere Unternehmen darüber informieren, dass der Betroffene die Löschung aller Links, Kopien und Replikationen der Daten verlangt.

TÜV SÜD-Praxishinweis

Sie sollten bestehende Lösch- und Sperrkonzepte bereits vorhandener IT-Systeme sowie die bestehenden Auswahlkriterien für Neuanschaffungen überprüfen. Die Vorkehrungen zum Schutz von Kindern verlangen zukünftig, personenbezogene Daten von Kindern als solche erkennen zu können. Sie sollten heute bereits entsprechende Informationsprozesse etablieren, bzw. die internen Betriebsabläufe – wenn möglich – derart ausrichten, dass es zu keinen derartigen Datenveröffentlichungen kommt.

1.8 Recht auf Datenübertragbarkeit, Art. 20

Die EU-DSGVO verpflichtet Unternehmen zukünftig, die Daten eines Betroffenen, die dieser dem Unternehmen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zurückzugeben. Diese Daten sind auf Wunsch des Betroffenen auch direkt an ein anderes Unternehmen zu übermitteln, soweit dies technisch machbar ist. Das Ende heterogener, unternehmensspezifischer Dateiformate europäischer Unternehmen ist damit zumindest auf dem Papier eingeläutet.

TÜV SÜD-Praxishinweis

Sie sollten prozessuale wie auch technische Vorkehrungen treffen, um Daten zukünftig übertragbar in Ihren IT-Systemen vorzuhalten. Dabei sollte bereits die Art der Datenerhebung überprüft werden, da die Übergabeverpflichtung alle Daten des Betroffenen umfasst.

1.9 Verantwortung des für die Verarbeitung Verantwortlichen, Art. 24

Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen, dass personenbezogene Daten in Übereinstimmung mit der EU-DSGVO verarbeitet werden. Dabei muss eine Überprüfung und ggf. Aktualisierung der technischen und organisatorischen Maßnahmen erfolgen. Höhere Hürden sind: Der für die Verarbeitung Verantwortliche muss im Vorfeld die Eintrittswahrscheinlichkeit und Schwere der Risiken für die persönlichen Rechte und Freiheiten der Betroffenen festlegen. Zudem muss er einen Nachweis dafür erbringen, dass personenbezogene Daten in Übereinstimmung mit der Verordnung verarbeitet werden. Es wird demnach eine (dokumentierte) Risikobetrachtung erforderlich sein, die anhand einer objektiven Bewertung beurteilt, welchen Risiken die Datenverarbeitung ausgesetzt ist und wie hoch das jeweilige Risiko eingeschätzt wird. Dabei können Ursache, Art, Eintrittswahrscheinlichkeit und Schwere als Kriterien heran-

gezogen werden. Spannend dürfte in diesem Zusammenhang sein, ob diese Risiken bzw. deren Eintrittsfall überhaupt erkannt werden (z. B. Cyberangriff).

TÜV SÜD-Praxishinweis

Es wird ein erheblicher Mehraufwand durch eine dokumentierte Darstellung der Eintrittswahrscheinlichkeit und Schwere der Risiken für die persönlichen Rechte der Betroffenen entstehen. Schaffen Sie zusätzliche Ressourcen in zeitlicher und finanzieller Hinsicht.

1.10 Datenschutzfreundliche Voreinstellungen, Art. 25

Unternehmen sind zukünftig zu datenschutzfreundlichen Voreinstellungen verpflichtet. Sie müssen sowohl zum Zeitpunkt der Konzeption wie auch der eigentlichen Datenverarbeitung geeignete technische und organisatorische Maßnahmen vorsehen, so dass durch entsprechende Voreinstellungen grundsätzlich nur personenbezogene Daten verarbeitet werden, die für den Verarbeitungszweck erforderlich sind. Diese Verpflichtung erfasst sowohl die Menge der erhobenen personenbezogenen Daten, wie auch den Umfang ihrer Verarbeitung, deren Speicherfrist und Zugänglichkeit.

TÜV SÜD-Praxishinweis

Entsprechende technische und organisatorische Maßnahmen sollten Ihrerseits getroffen werden. Zudem sollten bestehende IT-Systeme (insbesondere eigene Softwareprodukte und Apps) auf diese Datenschutzanforderung hin überprüft werden.

1.11 Auftragsverarbeitung, Art. 28 und gemeinsame Verantwortliche, Art. 26

Mit der neuen EU-DSGVO müssen Betriebe künftig umdenken, da aus der bekannten Auftragsdatenverarbeitung nunmehr die „Auftragsverarbeitung“ wird. Viele der Anforderungen, die 2009 mit der Gesetzesnovellierung eingeführt wurden, finden sich auch in der EU-DSGVO wieder. Neu ist jedoch die ausdrückliche Forderung nach Garantien auf Seiten des Auftragsverarbeiters. Auch die Möglichkeit, den bislang schriftlich abzuschließenden Vertrag zukünftig elektronisch abschließen zu können, ist eine Änderung, die die EU-DSGVO mit sich bringt. Der gesetzliche Anforderungskatalog an die zu treffenden inhaltlichen Regelungen fordert neue, über das heute in Deutschland bekannte Maß hinausgehende inhaltliche Absprachen.

Daneben bringt die EU-DSGVO eine „neue Form“ der arbeitsteiligen Zusammenarbeit zweier verantwortlicher Stellen. Auch wenn diese Art der Zusammenarbeit längst in der bisherigen Datenschutzrichtlinie angelegt war, hat sie es bis heute in dieser Klarheit nicht in das deutsche Bundesdatenschutzgesetz geschafft. Zukünftig können verantwortliche Stellen auch ohne Weisungserfordernis gemeinschaftlich Zusammenarbeiten, wenn sie die gemeinsamen Zwecke und die Verarbeitungsmittel gemeinsam vorgelagert festlegen. Die Vereinbarung muss in transparenter Form zu erfolgen und Auskunft darüber geben, welcher verantwortlichen Stelle welche Aufgabe obliegt. Dabei muss vor allem auf die Informationspflichten sowie die Realisierung der Wahrnehmung der Rechte der Betroffenen eingegangen werden.

TÜV SÜD-Praxishinweis

Überprüfen Sie die bestehenden Auftragsverarbeitungen und passen Sie die vertragliche Grundlage an die neuen Anforderungen an. Ferner sollten Sie bestehende Kooperationen dahingehend überprüfen, ob nicht die gemeinschaftliche Zusammenarbeit die für beide Seiten bessere Alternative darstellt.

1.12 Benachrichtigungspflichten bei Datenschutzverletzungen, Art. 33

Was bislang als Fall des § 42a BDSG bekannt war und eine Informationspflicht bei unrechtmäßiger Kenntniserlangung bestimmter personenbezogenen Daten nach sich gezogen hat, wird auch in der EU-DSGVO geregelt. Es besteht eine Benachrichtigungspflicht des Betroffenen, wenn dessen personenbezogene Daten verletzt werden und voraussichtlich zu einem Risiko für die Rechte und Freiheiten des Betroffenen führen. Der Betroffene muss ohne unangemessene Verzögerung und in klarer und einfacher Sprache

- über die Art der Verletzung,
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten, sowie
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Eindämmung ihrer möglichen nachteiligen Auswirkungen

informiert werden.

Neu ist, dass der Verantwortliche innerhalb von 72 Stunden nachdem die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde hierüber eine Meldung abgeben muss, die wiederum bestimmte Voraussetzungen erfüllen muss.

TÜV SÜD-Praxishinweis

Entwickeln Sie Prozesse, so dass Datenschutzverletzungen innerhalb der vorgegebenen Frist und mit den erforderlichen Angaben gemeldet werden können. Dokumentieren Sie die Verletzungen und welche Maßnahmen zur Abhilfe getroffen werden müssen. Schulen Sie Ihre Mitarbeiter, so dass Datenschutzverletzungen erkannt werden und rechtzeitig gemeldet werden! Ziehen Sie aus vergangenen Verletzungen Maßnahmen zur Optimierung der Prozesse!

1.13 Sicherheit der Verarbeitung, Art. 32

Der risikobasierende Ansatz der EU-DSGVO verpflichtet Unternehmen auch zukünftig zur Umsetzung von geeigneten technischen und organisatorischen Maßnahmen, mit denen ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Hierbei sind nicht nur der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und der Verarbeitungszweck der personenbezogenen Daten zu berücksichtigen, sondern auch die Eintrittswahrscheinlichkeit des Risikos und die Schwere eines solchen Risikos für die Betroffenenrechte sind maßgebend.

Die EU-DSGVO fordert explizit den technischen Einsatz von Pseudonymisierung und Verschlüsselung. Ferner müssen Vorkehrungen hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme getroffen werden. Unternehmen haben die rasche Wiederherstellung des Zugangs zu Daten im Fall eines physischen oder technischen Zwischenfalls genauso sicherzustellen, wie sie Regelprozesse etablieren müssen, um regelmäßig eine Bewertung und Evaluierung der Wirksamkeit bestehender technischer und organisatorischer Maßnahmen vorzunehmen.

TÜV SÜD-Praxishinweis

Überprüfen sie in diesem Kontext die heute bestehenden Maßnahmen auf Übereinstimmung mit den Anforderungen der EU-DSGVO. Prozessual sollten Sie Vorkehrungen treffen, die Ihnen eine regelmäßige Überprüfung und die damit einhergehende Dokumentation auch für die Zukunft sicherstellen.

1.14 Datenschutz-Folgenabschätzung, Art. 35

Die zukünftige Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung ist neu, bzw. zumindest als umfassende Weiterentwicklung der bislang bekannten Vorabkontrolle zu verstehen. Sie war immer dann durchzuführen, wenn die angedachten Datenverarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufgewiesen haben.

In Zukunft betrifft diese Verpflichtung alle Datenverarbeitungen und den gesamten Lebenszyklus der Datenverarbeitung. Insbesondere trifft dies bei der Verwendung neuer Technologien zu, die aufgrund der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen zur Folge haben. Die neue Datenschutz-Folgenabschätzung bedarf einer systematischen Beschreibung der geplanten Verarbeitungsvorgänge und der Verarbeitungszwecke, gegebenenfalls einschließlich der vom Unternehmen verfolgten berechtigten Interessen, einer Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck, sowie einer Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen.

TÜV SÜD-Praxishinweis

Passen Sie den Prozess der Vorabkontrolle an die neuen Anforderungen an und setzen Sie diese in dem nun geforderten breiten Anwendungsspektrum um. Hierfür sind Ihrerseits insbesondere prozessuale Anpassungen erforderlich. Zudem sollten Sie bestehende Vorabkontroll-Checklisten und Dokumentationen inhaltlich anzupassen.

1.15 Aufgaben und Pflichten des Datenschutzbeauftragten, Art. 37ff.

Die EU-DSGVO stellt es den Mitgliedstaaten – von einigen wenigen Ausnahmen abgesehen – hinsichtlich privatwirtschaftlicher Unternehmen frei, ob zukünftig die Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht. Nach aktuellem Diskussionsstand wird zumindest in Deutschland diese Verpflichtung Bestand haben.

Ist ein Datenschutzbeauftragter zu bestellen, so finden sich zahlreiche heute in Deutschland bereits geregelte Ansätze wieder. Der Datenschutzbeauftragte ist weisungsfrei, darf nicht abberufen oder benachteiligt werden und er ist der unmittelbar höchsten Managementebene zu unterstellen. Zu seinen Aufgaben zählt die Unterrichtung und Beratung des Unternehmens.

Neu ist jedoch die Pflicht zur Überwachung der Einhaltung der EU-DSGVO, anderer Datenschutzvorschriften sowie der Strategie des Unternehmens einschließlich der Zuweisung von Zuständigkeiten. Dies stellt eine ganz wesentliche Erweiterung des bislang bekannten Aufgaben- und Pflichtenbereichs eines Datenschutzbeauftragten dar.

TÜV SÜD-Praxishinweis

Sie sollten sich als Datenschutzbeauftragter mit den weiteren Entwicklungen beschäftigen und die nationale deutsche Gesetzgebung in diesem Kontext verfolgen. Das zu erwartende, weitere Aufgabenspektrum bringt mit den neuen Aufgaben auch einen zu vermutenden weiteren Haftungsrahmen, den Datenschutzbeauftragte in ihrem Alltag beachten sollten.

1.16 Zertifizierungen, Art. 42

Datenschutzspezifische Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen werden mit In-Krafttreten der EU-DSGVO von großer Bedeutung sein. Sie sollen einen Nachweis dafür geben, dass die Verordnung eingehalten wird. Diese Formulierung in der EU-DSGVO hätte allerdings zur Folge, dass tatsächlich bescheinigt werden müsste, dass sämtliche Regelungen der Verordnung eingehalten werden. Inwieweit hierzu noch Regelungsbedarf nötig ist und nach welchen Kriterien solche Zertifizierungen vergeben werden, ist noch unklar. Eine Zertifizierung durch akkreditierte Zertifizierungsstellen oder durch die zuständige Aufsichtsbehörde wird anhand genehmigter Kriterien erteilt werden.

TÜV SÜD-Praxishinweis

Stellen Sie zeitliche und finanzielle Ressourcen sicher, um Zertifizierungsverfahren durchführen und regelmäßig aktualisieren zu können. Stellen Sie im Vorfeld sicher, dass Sie die Einhaltung der EU-DSGVO nachweisen können.

1.17 Internationale Datenübermittlung, Art. 44ff.

Für eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation gilt wie bislang auch: Wurde durch die Kommission festgestellt, dass ein angemessenes Schutzniveau gegeben ist, ist eine Datenübermittlung ohne besondere Genehmigung möglich. Sollte ein angemessenes Schutzniveau nicht vorliegen, können die bekannten Instrumente wie Standardvertragsklauseln, Binding Corporate Rules oder die Einwilligung des Betroffenen herangezogen werden. Gerade hinsichtlich der Binding Corporate Rules ist begrüßenswert, dass die entsprechenden Voraussetzungen in der EU-DSGVO nunmehr aufgelistet sind. Insgesamt wurden die Entscheidungsgrundsätze des Safe Harbor-Urteils vom Oktober 2015 mit in die EU-DSGVO aufgenommen.

TÜV SÜD-Praxishinweis

Stellen Sie zusammen, welche Datenübermittlungen ins Ausland an welchen Rechtsgrundlagen geknüpft sind und prüfen Sie, inwieweit ein angemessenes Datenschutzniveau erreicht wird. Überprüfen Sie in jedem Fall die heute bestehenden Vertragsdokumente.

1.18 Haftung und Recht auf Schadensersatz, Art. 82

Die heutigen Regelungen des Bundesdatenschutzgesetzes verpflichten Unternehmen zum Schadensersatz, wenn dem Betroffenen ein materieller Schaden entstanden ist und dieser aus einer unzulässigen oder unrichtigen Datenverarbeitung entstanden ist. Dies gilt zumindest immer dann, wenn die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt nicht beachtet hat.

Die EU-DSGVO erweitert zukünftig die Haftungsverantwortlichkeit eines jeden Unternehmens und verpflichtet ergänzend auch im Fall von rein moralischen Schäden zur Schadensersatzpflicht. Zukünftig wird nicht mehr nur überprüft werden, ob ein Schaden tatsächlich in der vorgeworfenen Datenverarbeitung seine Ursache gefunden hat, sondern ob die Datenverarbeitung einer zu erwartenden sachgerechten Datenverarbeitung entsprochen hat. Damit steigt das potentielle Haftungsrisiko eines jeden Unternehmens.

TÜV SÜD-Praxishinweis

Überprüfen Sie die bestehenden Datenverarbeitungsprozesse anhand der neuen Erlaubnistatbestände der EU-DSGVO auf deren weiterhin bestehende Rechtmäßigkeit. Ferner sollten Sie eine Neubewertung bestehender Haftungsrisiken vornehmen und die erweiterten Haftungsrahmen in heutige Geschäftsprozesse wie auch zukünftige Projektplanungen einfließen lassen.

1.19 Haftungserstreckung auf ausländische Unternehmen, Art. 3

Die Haftung der EU-DSGVO trifft nun mehr auch ausländische Unternehmen, selbst wenn diese keine Filiale in einem Mitgliedstaat der Europäischen Union unterhalten (sog. Marktortprinzip). Für diese Haftungserstreckung ist lediglich erforderlich, dass die Datenverarbeitung dazu dient, Unionsbürgern Waren oder Dienstleistungen anzubieten bzw. deren Verhalten zu beobachten, soweit dieses Verhalten in der Europäischen Union erfolgt. Damit haftet neben Facebook, Google und Co. zukünftig jeder Warenverkäufer und Diensteerbringer, sofern er sich mit seinem Angebot in einer Sprache der Europäischen Union an Unionsbürger richtet.

TÜV SÜD-Praxishinweis

Machen Sie sich mit den völlig neuen Spielregeln vertraut, auch wenn Sie als Verantwortlichereines ausländischen Unternehmens aufgrund fehlender Filialen in der Europäischen Union bislang keine Haftung zu erwarten hatten.

1.20 Bußgelder und Sanktionen, Art. 83ff.

Der heute bekannte Bußgeldrahmen für Unternehmen beläuft sich je nach Schwere des Verstoßes auf bis zu 50.000 Euro bzw. 300.000 Euro.

Die EU-DSGVO bringt vor allem in diesem Kontext einschneidende Neuerungen. Bereits der Gesetzestext legt den Aufsichtsbehörden die Verpflichtung auf, zukünftig „abschreckende" Bußgeldhöhen zu verhängen. Damit sind die Zeiten, in denen Bußgelder eingepreist oder ignoriert werden konnten, in der Zukunft vorbei.

Der Bußgeldrahmen der EU-DSGVO beläuft sich je Schwere des Verstoßes auf 10.000.000 Euro bzw. 20.000.000 Euro oder im Fall eines Unternehmens auf bis zu 2 % bzw. 4 % des gesamten weltweit erzielten Jahresumsatzes des vorgelagerten Geschäftsjahres.

TÜV SÜD-Praxishinweis

Überprüfen Sie bestehende Datenverarbeitungsprozesse auf deren weiterhin bestehende Rechtmäßigkeit. Zudem empfehlen wir Ihnen als verantwortliche Stelle dringend, eine Neubewertung bestehender Haftungsrisiken vorzunehmen und die erweiterten Haftungsrahmen in heutige Geschäftsprozesse wie auch zukünftige Projektplanungen einfließen zu lassen.

2. Zusammenfassung und Ausblick

Die EU-DSGVO wird das Bundesdatenschutzgesetz am 25.05.2018 beinahe ganzheitlich ersetzen und für die Unternehmen „neue Spielregeln“ aufstellen. Die Neuerungen treffen jedes Unternehmen jeder Branche und fordern in einer nur kurzen Umsetzungszeit, dass der Bereich Datenschutz von jedem Unternehmen in seiner Gesamtheit überprüft und gegebenenfalls angepasst wird.

Alle Unternehmen sind nun gefordert, bestehende Datenverarbeitungen zu überprüfen und zahlreiche neue Prozesse zu schaffen. Selbst bereits etablierte Datenschutzorganisationen müssen neu durchdacht und an die neuen Anforderungen angepasst werden.

Daneben sind existierende Muster, Checklisten und Vertragsdokumente zu überarbeiten. Datenschutzgrundsätze wie beispielsweise „Datenschutz durch Technik (data protection by design)“ und „datenschutzfreundliche Voreinstellungen (data protection by default)“ treten nun mehr neben die erweiterten Anforderungen einer „Datenschutz-Folgenabschätzung (data protection impact assessment)“ und fordern angepasste technische und organisatorische Maßnahmen.

Diese White Paper-Reihe wird Ihnen die wichtigsten Änderungen aufzeigen und Sie über die neuesten Entwicklungen auf dem Laufenden halten.

Akademie

Wissen, worauf es ankommt

www.tuev-sued.de/akademie

Ihr Ansprechpartner bei der TÜV SÜD Akademie:

Uwe Laubner
Fachliche Leitung Datenschutz

Tel. +49 (0)89 5791-2388
E-Mail: akd.datenschutz-seminare@tuev-sued.de

Ihr Ansprechpartner bei der TÜV SÜD Sec-IT:

Florian Labitzke
Produktmanager Datenschutz

Tel. +49 (0)89 500 84-300
E-Mail: florian.labitzke@tuev-sued.de

Die Autoren

RAin Doris Brandl
Frau Doris Brandl ist Rechtsanwältin und zertifizierte Datenschutzbeauftragte. Sie ist bei der TÜV SÜD Sec-IT GmbH in München als Fachexpertin im Bereich Datenschutz tätig und berät bundesweit zu datenschutzrechtlichen Fragestellungen. Darüber hinaus übernimmt Frau Brandl die Funktion der externen Datenschutzbeauftragten.

Sie ist Mitherausgeberin des „Elektronischen Datenschutzhandbuchs", veröffentlicht regelmäßig Fachbeiträge und referiert zu aktuellen Themen im Bereich Datenschutz.

RA Markus Säugling
Herr Markus Säugling ist Rechtsanwalt, Datenschutzauditor, ISO/IEC 27001 Lead Auditor sowie zertifizierter, für zahlreiche Unternehmen tätiger externer Datenschutzbeauftragter. Er ist Gründungspartner des Beratungsunternehmens MAGELLAN, das sich als Beratungsunternehmen und Rechtsanwaltskanzlei auf die Bereiche Datenschutz, Informationstechnologie und IT-Sicherheit spezialisiert hat. Es berät sowohl mittelständische Unternehmen als auch namhafte Konzerne.

Herr Säugling ist der Herausgeber und Autor des Systematischen Praxiskommentars Datenschutzrecht: Datenschutz aus Unternehmenssicht. Ferner ist er Autor des TÜV SÜD Akademie-Ausbildungskurses „Datenschutzbeauftragter DSB-TÜV" sowie Dozent der TÜV SÜD Akademie.

Herr Säugling war viele Jahre als Konzerndatenschutzbeauftragter für den größten europäischen Kabelnetzbetreiber sowie eines der weltweit führenden Pharmaunternehmen tätig.
(www.magellan-datenschutz.de)

Dieses White Paper entstand in Kooperation mit der TÜV SÜD Sec-IT GmbH.
Die TÜV SÜD Sec-IT bündelt mit ihren innovativen Leistungen Kompetenzen der Bereiche IT-Security und Datenschutz.
Weitere Informationen zur TÜV SÜD Sec-IT finden Sie unter: www.tuev-sued.de/fokus-themen/it-security

TÜV SÜD Akademie GmbH
Westendstraße 160
80339 München

Bleiben wir in Kontakt!