

Die neue europäische Datenschutz-Grundverordnung (EU-DSGVO): Was ändert sich für Spanien?

Die neue EU-DSGVO trat bereits am 25. Mai 2016 in Kraft. Sie sieht jedoch eine Übergangszeit von zwei Jahren vor und gilt damit erstmals ab dem 25. Mai 2018 verbindlich für die Mitgliedsstaaten der Europäischen Union. Bis dahin bleiben sowohl die bisherige Datenschutzrichtlinie 95/46 als auch die nationalen spanischen Normen, die diese umsetzen, gültig und anwendbar. Durch die EU-DSGVO wird letztlich das „Ley Orgánica de Protección de Datos 1999/15“ (LOPD) ersetzt und eine Vereinheitlichung des Datenschutzes innerhalb der EU herbeigeführt. Der räumliche Anwendungsbereich der EU-DSGVO erstreckt sich nach dem sog. „Marktortprinzip“ aber auch auf außereuropäische Unternehmen, sofern sie am europäischen Markt tätig sind.

Für Spanien hält die EU-DSGVO einige Änderungen, aber auch Neuerungen bereit. Im Vordergrund stehen dabei vor allem präventive Gesichtspunkte. So etabliert sie ein sogenanntes *proaktives Verantwortlichkeitsprinzip*. Das bedeutet, dass die Verantwortlichen - also die Unternehmen - im Voraus Maßnahmen ergreifen müssen, um zu gewährleisten, dass sie die in der Verordnung festgelegten Grundsätze, Rechte und Garantien einhalten. Vor dem Hintergrund dieser proaktiven Verantwortlichkeit ist es gerade nicht mehr ausreichend, erst zu handeln, wenn schon eine Verletzung des Datenschutzes eingetreten ist, da dies zu schwer kompensierbaren Schäden führen kann. Zu diesem Zweck sieht die EU-DSGVO eine Reihe von Maßnahmen vor:

- Datenschutz durch Technik
- datenschutzfreundliche Voreinstellungen
- Sicherheitsmaßnahmen
- Führen eines Verzeichnisses über die Datenverarbeitung
- Durchführung von Folgenabschätzungen zum Datenschutz
- Benennung eines Datenschutzbeauftragten
- Benachrichtigung über Verstöße gegen den Datenschutz
- Förderung des Verhaltenskodexes und der Zertifizierungssysteme

Im Folgenden werden die grundlegenden Änderungen näher erläutert und Hinweise für die Praxis erteilt.

Eine wichtige Änderung ist im Bereich der Einwilligung in den Datenverarbeitungsvorgang vorgenommen worden. So kann die freiwillige Einwilligung in die Datenverarbeitung durch die betroffene Person nur erfolgen, wenn sie diese eindeutig und unmissverständlich erklärt. Dies könnte etwa durch (aktives) Anklicken eines Kästchens beim Besuch einer Internetseite geschehen. Konkludente Einwilligungen (bspw. bereits angekreuztes Kästchen) und solche durch Unterlassen



AHK

Deutsche Handelskammer
für Spanien
Cámara de Comercio Alemana
para España

wie sie das spanische nationale Recht im LOPD noch als zulässig ansieht, sind demnach nicht mehr möglich.

Daneben werden an die Einwilligung beim Umgang mit sensiblen Daten, bei automatisierten Vorgängen und bei internationalen Überweisungen strengere Anforderungen gestellt. Hier kann die Einwilligung nicht durch (irgendeine) aktive Handlung erfolgen. Erforderlich ist vielmehr, dass sich die Handlung ausdrücklich auf die Zustimmung zur Datenverarbeitung bezieht.

Eine Einwilligung durch einen Minderjährigen ist grundsätzlich ab dem 16. Lebensjahr rechtmäßig. Zuvor ist die Verarbeitung nur rechtmäßig, sofern und soweit die Einwilligung durch die Eltern oder mit deren Zustimmung erteilt wird. Die Mitgliedstaaten können jedoch durch Rechtsvorschriften zu diesen Zwecken eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem vollendeten 13. Lebensjahr liegen darf. In Spanien sieht das LOPD eine Einwilligung zur Datenverarbeitung ab dem 14. Lebensjahr als wirksam an. Für Unternehmen, hat das zur Folge, dass die vorformulierte Zustimmung nachvollziehbar und die Datenschutzerklärung so geschrieben sein muss, dass sie auch von Minderjährigen verstanden werden kann.

Hinsichtlich der Informationsbereitstellung soll der Verantwortliche die übermittelten Informationen in einer prägnanten, transparenten, verständlichen und einfachen Weise mit klarer und einfacher Sprache fassen. Dies dürfte in der Praxis vor dem Hintergrund der Komplexität des Datenschutzes eine Herausforderung darstellen.

Eine wichtige Änderung ermöglicht es zudem, dass die Person, die von dem Verantwortlichen Auskunft verlangt, nunmehr unentgeltlich eine *Kopie* der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, verlangen kann. Nach dem LOPD sind die verarbeiteten Daten lediglich vorzulegen. Eine Aushändigung einer Kopie ist – außer im Fall von Daten, die den Krankheitsverlauf der Auskunft ersuchenden Person betreffen, – nicht vorgesehen.

Neben den traditionellen ARCO Rechten (acceso, rectificación, cancelación y oposición = Zugang, Berichtigung, Sperrung, Einspruch) enthält die EU-DSGVO auch neue Betroffenenrechte. So steht dem Betroffenen nun als Manifestation der Widerrufsrechte das „Recht auf Vergessenwerden“ zu. Dieses Recht ermöglicht es dem Nutzer unter bestimmten Bedingungen, dass Links aus Suchmaschinen verschwinden und ihn betreffende persönliche Informationen, die veraltet, unvollständig, falsch oder irrelevant und unter anderem nicht von öffentlichem Interesse sind, gesperrt werden und somit nicht mehr öffentlich im Internet abrufbar sind.

Des Weiteren kann der Verantwortliche auch die Einschränkung der Verarbeitung verlangen, wenn die dafür vorgesehenen Voraussetzungen des Art. 18 Abs. 1 EU-



AHK

Deutsche Handelskammer
für Spanien
Cámara de Comercio Alemana
para España

DSGVO vorliegen. Dieses Recht steht nur dem Betroffenen zu und darf nicht mit der Möglichkeit der Datensperre im LOPD verwechselt werden. Als erweiterte Form des Auskunftsrechts ermöglicht das Recht auf Datenübertragbarkeit dem Betroffenen seine Daten einem anderen, dritten Verantwortlichen zu übermitteln, wenn die Verarbeitung mithilfe automatisierter Verfahren erfolgt und/oder die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht.

Die Verantwortlichen, also die Unternehmen, sollen die – grundsätzlich kostenlose – Ausübung dieser Rechte vereinfachen und sichtbare, zugängliche und verständliche Formulare hierfür bereitstellen.

Drei Neuerungen ergeben sich auch im Verhältnis Verantwortlicher – Auftragsverarbeiter.

- Die EU-DSGVO beinhaltet nunmehr ausdrücklich Pflichten für die Auftragsverarbeiter. So müssen sie – ggf. auch ihre Vertreter – beispielsweise ein Verzeichnis führen, das die Verarbeitungstätigkeit dokumentiert. Die Auftragsverarbeiter können auch von den Datenschutzbehörden gesondert überwacht werden.
- Während das LOPD die Notwendigkeit einer Due Diligence bei der Auswahl Auftragsverarbeiter festlegt, sollen die Verantwortlichen nach der EU-DSGVO nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen.
- Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsakts, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet. Vertraglich sollen Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt werden. In der Praxis hat dies zur Folge, dass die Verträge, die vor der Anwendung EU-DSGVO im Mai 2018 abgeschlossen wurden, gegebenenfalls modifiziert und angepasst werden müssen.

Neben dem proaktiven Verantwortungsprinzip führt die EU-DSGVO auch einen *Risikoansatz* ein, der von den Verantwortlichen und auch von den Auftragsverarbeiter angewendet werden soll. Zunächst sollen im Rahmen einer objektiven Risikobewertung Eintrittswahrscheinlichkeit und Schwere von Eingriffen in Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Zusätzlich soll jeder Verantwortliche und Auftragsverarbeiter ein Verzeichnis aller Verarbeitungstätigkeiten führen. Diese Pflicht gilt jedoch nicht für Unternehmen oder Einrichtungen, die weniger als 250

Mitarbeiter beschäftigen, es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 EU-DSGVO bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 EU-DSGVO.

Nach dem in der EU-DSGVO verankerten *proaktiven Verantwortungsprinzip* müssen die Verantwortlichen im Hinblick auf die Datenverarbeitung geeignete technische und organisatorische Maßnahmen ergreifen. Dabei sollen bei der Auswahl der Maßnahmen im Gegensatz zur LOPD nun *mehrerer Variablen* berücksichtigt werden, nämlich der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen. Die Maßnahmen sollen insbesondere den Grundsätzen des Datenschutzes durch Technik (*protección de datos desde el diseño*) und durch datenschutzfreundliche Voreinstellungen (*protección de datos por defecto*) entsprechen. In Betracht kommt beispielsweise eine Minimierung der Verarbeitung personenbezogener Daten, eine Pseudonymisierung personenbezogener Daten und die Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten. Geht jedoch aus einer Datenschutz-Folgenabschätzung hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das der Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so sollte die Aufsichtsbehörde vor der Verarbeitung informiert werden. Ist es hingegen schon zu einer Verletzung des Datenschutzes gekommen, muss der Verantwortliche die zuständige Datenschutzbehörde unverzüglich und binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, benachrichtigen, es sei denn, es ist unwahrscheinlich, dass die Verletzung ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt. Erfolgt die Meldung nicht innerhalb dieses Zeitraums, so ist ihr eine Begründung für die Verzögerung beizufügen.

Der Verantwortliche und der Auftragsverarbeiter haben zudem unter den Voraussetzungen des Art. 37 Abs. 1 EU-DSGVO einen Datenschutzbeauftragten zu benennen. Eine Unternehmensgruppe kann einen gemeinsamen Datenschutzbeauftragten ernennen, sofern Datenschutzbeauftragte von jeder Niederlassung aus leicht erreicht werden kann. Die Auswahl des Datenschutzbeauftragten erfolgt auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 EU-DSGVO genannten Aufgaben. Er kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder aber aufgrund eines

Dienstleistungsvertrags tätig werden. Zudem sollten Datenschutzbeauftragte ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.

Nach alledem scheinen einige Lücken im Datenschutzrecht durch die neue EU-DSGVO geschlossen. Für die Unternehmen bedeutet dies zunächst, dass sie ihre Datenschutzerklärungen überprüfen sollten. Diese muss nunmehr die Rechtsgrundlage für die Verarbeitung der Daten enthalten, die Aufbewahrungsfristen der Daten nennen und auf die Möglichkeit der Beschwerde bei der Datenschutzbehörde hinweisen. Diese Informationen sollten leicht verständlich und präzise dargestellt werden. Daneben sollte eine möglichst zeitnahe Modifizierung der bisherigen Arbeitsabläufe und Prozesse sowie der IT-Systeme und Strukturen der Datenverarbeitung erfolgen, um die Wahrung der Verordnung zu gewähren. Dies wird insbesondere für kleinere Unternehmen auch eine finanzielle Herausforderung sein.

Weitere Informationen und einen Leitfaden für die neue EU-DSGVO finden Sie auch auf der Webseite der Agencia Española de Protección de Datos unter folgendem Link:
http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

**AHK**Deutsche Handelskammer
für Spanien
Cámara de Comercio Alemana
para España

Spanisches Datenschutzrecht nach dem „Ley Orgánica de Protección de Datos 1999/15“ (LOPD)	Europäische Datenschutz-Grundverordnung (EU-DSGVO)
<p>Die <i>Einwilligung</i> in die Datenverarbeitung kann nach spanischem Recht bereits <i>konkludent oder durch Unterlassen</i> erfolgen (Bsp. Bereits angeklicktes Kästchen in Webfenstern). Ein ausdrückliches Handeln ist demnach nicht erforderlich.</p>	<p>Die <i>Einwilligung</i> in die Datenverarbeitung muss eindeutig und unmissverständlich erklärt werden, d.h. nur durch <i>aktives Tun</i>. Eine konkludente Einwilligung oder eine solche durch Unterlassen ist nicht mehr möglich, da dies auf völliger Untätigkeit beruht.</p> <p>Daneben muss das Einverständnis beim Umgang mit sensiblen Daten, bei automatisierten Vorgängen sowie internationalen Überweisungen nicht nur eindeutig, sondern auch <i>explizit</i> erfolgen.</p>
<p>Die Einwilligung in den Datenverarbeitungs-vorgang ist ab dem 14. Lebensjahr als wirksam anzusehen.</p>	<p>Zwar sieht die EU-DSGVO eine Einwilligung durch einen Minderjährigen erst ab dem 16. Lebensjahr als wirksam an, jedoch ermöglicht sie auch eine anderweitige Regelung durch die Mitgliedsstaaten. Dabei darf aber eine Altersgrenze von 13 Jahren nicht unterschritten werden.</p> <p>Grundsätzlich hat diese Regelung also keine Änderung für Spanien zur Folge.</p>
<p>Das LOPD verlangt nur, dass die Informationen <i>genau, präzise und unmissverständlich</i> zur Verfügung gestellt werden.</p>	<p>Die Informationsbereitstellung soll in einer <i>prägnanten, transparenten und leicht verständlichen Weise mit klarer und einfacher Sprache</i> erfolgen.</p>
<p>Hinsichtlich des Auskunftsrechts sind die verarbeiteten Daten der ersuchenden Person lediglich vorzulegen. Eine Aushändigung einer <i>Kopie</i> ist <i>nicht vorgesehen</i>. Dies gilt aber nicht, wenn die eingesehenen Daten den</p>	<p>Im Rahmen des Auskunftsrechts erhält die ersuchende Person nunmehr von dem Verantwortlichen <i>eine Kopie</i> der personenbezogenen Daten, die Gegenstand der Verarbeitung sind</p>



AHK

Deutsche Handelskammer
für Spanien
Cámara de Comercio Alemana
para España

<p>Krankheitsverlauf betreffen. In diesem Fall wird eine Kopie angefertigt.</p>	
<p>Eine vorherige <i>Einschränkbarkeit</i> der <i>Verarbeitung</i> existiert nicht. Es besteht lediglich die Möglichkeit die personenbezogenen Daten sperren zu lassen.</p>	<p>Die EU-DSGVO enthält neben den traditionellen "ARCO Rechten" (acceso, rectificación, cancelación y oposición = Zugang, Berichtigung, Sperrung, Einspruch) auch neue Betroffenenrechte:</p> <ul style="list-style-type: none">- Das "<i>Recht auf Vergessenwerden</i>" ermöglicht es dem Nutzer unter bestimmten Bedingungen, dass Links aus Suchmaschinen verschwinden und ihn betreffende persönliche Informationen, die veraltet, unvollständig, falsch oder irrelevant und unter anderem nicht von öffentlichem Interesse sind, gesperrt werden und somit nicht mehr öffentlich im Internet abrufbar sind.- Der Verantwortliche kann nun auch die <i>Einschränkung der Verarbeitung verlangen</i>, wenn die Voraussetzungen des Art. 18 Abs. 1 EU-DSGVO vorliegen.- Das <i>Recht auf Datenübertragbarkeit</i> ermöglicht es dem Betroffenen, seine Daten einem anderen, dritten Verantwortlichen zu übermitteln, wenn die Verarbeitung mithilfe automatisierter Verfahren erfolgt und/oder die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht.
<p>Das LOPD und auch die RL 95/46 konzentrierten sich hinsichtlich der</p>	<p>Im Verhältnis Verantwortlicher - Auftragsverarbeiter ergeben sich durch</p>



AHK

Deutsche Handelskammer
für Spanien
Cámara de Comercio Alemana
para España

Pflichten auf die *Verantwortlichen* und ließen die Auftragsverarbeiter außer Betracht.

Nach dem LOPD ist die Auswahl eines Auftragsverarbeiters nach einer erfolgten *Due Diligence Prüfung* vorzunehmen.

die EU-DSGVO drei Neuerungen:

- Die EU-DSGVO beinhaltet nunmehr ausdrücklich *Pflichten für die Auftragsverarbeiter*. So müssen sie – ggf. auch ihre Vertreter – beispielsweise ein Verzeichnis führen, das die Verarbeitungstätigkeit dokumentiert. Die Auftragsverarbeiter können auch von den Datenschutzbehörden gesondert überwacht werden.
- Die Verantwortlichen sollen nach der EU-DSGVO nur *Auftragsverarbeiter* heranziehen, die – insbesondere im Hinblick auf *Fachwissen, Zuverlässigkeit* und *Ressourcen* – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen.
- Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der *Grundlage eines Vertrags oder eines anderen Rechtsakts*, der den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet. Vertraglich sollen Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt werden. Die Verträge, die vor der

	<p>Anwendung EU-DSGVO im Mai 2018 abgeschlossen wurden, müssen daher gegebenenfalls modifiziert und angepasst werden.</p>
	<p>Zudem wird in der EU-DSGVO auch ein <i>Risikoansatz</i> etabliert, d.h. im Rahmen einer objektiven Risikobewertung sollen zunächst Eintrittswahrscheinlichkeit und Schwere von Eingriffen in Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Zusätzlich soll jeder Verantwortliche und Auftragsverarbeiter ein Verzeichnis aller Verarbeitungstätigkeiten führen. Diese Pflicht gilt jedoch nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.</p>
<p>Das LOPD hat die Auswahl der zu ergreifenden Maßnahmen lediglich nach der <i>Art</i> der verarbeiteten Daten bestimmt.</p>	<p>Nach dem in der EU-DSGVO verankerten <i>Verantwortungsprinzip</i> müssen die Verantwortlichen im Hinblick auf die Datenverarbeitung geeignete technische und organisatorische Maßnahmen ergreifen. Dabei sollen bei der Auswahl der Maßnahmen <i>mehrere Variablen</i> berücksichtigt werden, nämlich der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände</p>

	<p>und die Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen. Als mögliche Maßnahmen kommen beispielsweise eine Minimierung der Verarbeitung personenbezogener Daten, eine Pseudonymisierung personenbezogener Daten und die Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten in Betracht. Geht jedoch aus einer Datenschutz-Folgenabschätzung hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das der Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so sollte die Aufsichtsbehörde vor der Verarbeitung informiert werden. Ist es hingegen schon zu einer Verletzung des Datenschutzes gekommen, muss der Verantwortliche die zuständige Datenschutzbehörde benachrichtigen, es sei denn, es ist unwahrscheinlich, dass die Verletzung ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.</p>
	<p>Der Verantwortliche und der Auftragsverarbeiter haben zudem unter den Voraussetzungen des Art. 37 Abs. 1 EU-DSGVO einen <i>Datenschutzbeauftragten</i> zu <i>benennen</i>. Die Auswahl erfolgt auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten</p>



Deutsche Handelskammer
für Spanien
Cámara de Comercio Alemana
para España

	Aufgaben.
--	-----------

Caterina Hanke – Rechtsreferendarin – AHK Spanien

Stand: 09/2017