ERSTE SCHRITTE IN RICHTUNG EU-DATENSCHUTZ-GRUNDVERORDNUNG

enterprise europe network
Wir stehen Unternehmen zur Seite

Die Europäische Datenschutz-Grundverordnung (DSGVO) trat am 25. Mai 2018 in Kraft. Sie bringt Verbrauchern neue Rechte und Unternehmen neue Pflichten. Doch womit sollte man als Unternehmen anfangen, wenn man die DSGVO erfüllen will?

Unter personenbezogene Daten fallen alle Informationen über die die Identität einer Person bestimmt werden kann (z.B. Name, Adresse, Telefonnummer, Email-Adresse, Personalnummer, Kfz-Kennzeichen, usw.).

KARTOGRAPHIEREN SIE IHRE KUNDEN- UND MITARBEITERDATEN

In einem ersten Schritt sollten Sie alle Vorgänge, in denen personenbezogene Daten in Ihrem Unternehmen verarbeitet oder gespeichert werden (z.B. Personalverwaltung, Erstellung einer Kundenakte, usw.) definieren und niederschreiben. Dokumentieren Sie für jeden Vorgang welche personenbezogenen Daten Sie besitzen, welche Zwecke die Verarbeitung hat, wo diese Daten gespeichert werden, welche Personen Zugang zu diesen haben und ob eine Datenvernichtung vorgesehen ist.

Stellen Sie sich anschließend in einem zweiten Schritt folgende Fragen:

? FRAGE	! ERKLÄRUNG
Sammle ich mehr Daten als ich benötige? Behalte ich die Daten länger als nötig?	Beachten Sie, dass Sie nur die unbedingt notwendigen Daten (und nicht die nützlichen Daten) sammeln und speichern **(Prinzip der Datenminimierung)**. Stellen Sie sich selbst folgende Fragen: Warum sammle ich diese Informationen? Benötige ich diese Daten, um mein Produkt oder meine Dienstleistung anzubieten? Ein weiterer Grundsatz den es zu respektieren gilt ist das **Prinzip der zeitlich begrenzten Aufbewahrung.** Um diesen Grundsatz zu erfüllen, sollten Sie sich vergewissern ob Sie einer gesetzlichen Aufbewahrungspflicht unterliegen (z.B. 10 Jahre für ausgestellte Rechnungen) oder nicht. Stellen Sie anschließend sicher, dass diese Daten sachlich richtig und auf dem neuesten Stand sind. Sollte dies nicht der Fall sein, müssen die falschen Daten gelöscht oder korrigiert werden. **(Prinzip der Datengenauigkeit).** Denn unter der DSGVO müssen aktive Maßnahmen ergriffen werden, um Informationen zu löschen, sobald sie ihre Relevanz verloren haben. Argumente wie z.B. „das könnte irgendwann mal nützlich sein" oder „man weiß ja nie" gelten unter der DSGVO demnach nicht. Die gesammelten Angaben dürfen nur zu dem Zweck verwendet werden, zu dem sie gesammelt wurden und dürfen nicht länger gespeichert werden als nötig.
Ist die Verarbeitung der personenbe-zogenen Daten rechtmäßig?	Die Verarbeitung von personenbezogenen Daten ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist **(Prinzip der Zulässigkeit)***: • Einhaltung rechtlicher Verpflichtung (Beispiel: gesammelte Daten für Steuer- und Sozialabgaben) • Erfüllung eines Vertrags sowie die Durchführung vorvertraglicher Maßnahmen (Beispiel: Verwaltung von Arbeitsverträgen, Erstellung von Angeboten) • Berechtigtes Interesse des für die Datensammlung Verantwortlichen (dieses Interesse darf die Rechte und Freiheiten der betroffenen Person jedoch nicht überwiegen) **Öffentliches Interesse sowie lebenswichtiges Interesse sind zwei weitere Bedingungen bei denen die Verarbeitung von personenbezogenen Daten rechtmäßig ist. Diese haben jedoch im Handwerk keine Relevanz.* Falls keiner von den obengenannten Gründen zur Datensammlung vorliegt, müssen Sie ein Einwilligungsschreiben von Ihren Kunden einholen. Stimmt die betroffene Person dieser Verarbeitung zu, muss sie dies durch eine aktive Handlung tun (z.B. durch Ankreuzen eines Auswahlfeldes). Dokumentieren Sie anschließend die Einwilligung, denn diese muss auf Anfrage nachgewiesen werden können.

FRAGE	ERKLÄRUNG
Ist die betroffene Person über die Datenverarbeitung informiert? Kann ich das Recht auf Berichtigung, Auskunft sowie Löschung respektieren?	Klären Sie in einer klaren und einfachen Sprache darüber auf, warum und welche personenbezogenen Daten Sie für wie lange verarbeiten und ob diese an Auftragsverarbeiter weitergeleitet werden **(Prinzip der Transparenz)**. Sie müssen sicherstellen, dass Sie auf Wunsch der betroffenen Person Auskunft über die gespeicherten Daten geben oder sie löschen können. Sobald Informationen über gespeicherte Daten angefordert werden, sollten Sie diese der betroffenen Person umgehend bereitstellen. Seien Sie deshalb darauf vorbereitet, wenn Ihre Kunden Sie fragen, welche Daten Sie über sie besitzen. Außerdem haben Personen das Recht gelöscht zu werden. Solange es jedoch gesetzliche Aufbewahrungspflichten gibt oder die Aufbewahrung der Daten zur Erfüllung eines Vertrages notwendig ist, müssen Sie diese nicht löschen. Sollte die Löschung aus technischen Gründen nicht möglich sein, sollten Daten anonymisiert werden, so dass die betroffene Person nicht mehr identifiziert werden kann, auch nicht von Ihnen selbst.
Sind meine personenbezogenen Daten sicher gelagert?	Die sichere Aufbewahrung von personenbezogenen Informationen liegt in Ihrer Verantwortung. Darunter fällt unter anderem auch das Übertragen Ihrer Kunden- bzw. Mitarbeiterdaten an Dritte (z.B. Lieferanten, externe Buchhaltung, Cloud-Anbieter). Letztendlich haben Sie die Verantwortung, dass mit den Daten nichts passiert. Stellen Sie deshalb sicher, dass Datenschutz sowie Datensicherheit bei Ihren Vertragspartnern genauso großgeschrieben werden wie bei Ihnen selbst. Tauschen Sie viele personenbezogene Daten mit Ihren Partnern aus, sollten Sie die Datenschutz- und Haftungsklauseln in Ihren Verträgen überprüfen. Wenn Ihnen eine Verletzung des Datenschutzes bekannt wird, die die Rechte und Freiheiten der betroffenen Personen gefährdet, müssen Sie diese innerhalb 72 Stunden der Nationalen Kommission für den Datenschutz (CNPD) melden.
Muss ich einen Datenschutzbeauftragten (DSB) ernennen?	Der DSB überwacht die Umsetzung und Einhaltung der DSGVO in Ihrem Unternehmen und dient als Ansprechpartner für alle Anfragen und Beschwerden betroffener Personen. Die Ernennung eines Datenschutzbeauftragten ist obligatorisch für: • öffentliche Einrichtungen • Unternehmen, deren Kerngeschäft eine regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang erfordert oder deren Kerngeschäft die Verarbeitung sensibler Daten ist. In allen anderen Fällen ist die Benennung eines DSB fakultativ.
Bin ich verpflichtet ein Verzeichnis der Verarbeitungstätigkeiten zu führen?	Die Erstellung des Verzeichnisses ist für kleinere Unternehmen mit weniger als 250 Angestellten nicht obligatorisch, es sei denn, die Verarbeitung von personenbezogenen Daten ist riskant, nicht gelegentlich oder es handelt sich um sensible oder rechtliche Daten. Doch auch wenn Sie als Unternehmen nicht dazu verpflichtet sind ein Verzeichnis der Verarbeitungstätigkeiten zu führen, erweist sich die Erstellung eines solchen auch für kleinere Unternehmen als sehr hilfreich da Sie sich so eine klare Übersicht aller Verarbeitungsvorgänge verschaffen können und so Ihrer Dokumentationspflicht nachgehen.

Die Nationale Kommission für den Datenschutz (CNPD) hat eine Broschüre zur Sensibilisierung der breiten Öffentlichkeit veröffentlicht. Das Ziel dieser Broschüre ist es den Bürgern ihre Rechte im Bereich des Datenschutzes näher zu bringen und ihnen zu erklären wie sie diese Rechte geltend machen können. Die Broschüre existiert in deutscher und französischer Fassung. Sie ist in gedruckter Form verfügbar und kann auf der Internetseite der CNPD (www.cnpd.lu) heruntergeladen werden.

CHAMBRE DES METIERS Luxembourg

YDÉ

Haben Sie noch Fragen? Möchten Sie weitere Informationen zu den bestehenden Angeboten erhalten? Dann zögern Sie nicht die Abteilung eHandwierk der Chambre des Métiers zu kontaktieren:

Tel.: 42 67 67 - 305 / 306 | **E-Mail:** ehandwierk@cdm.lu