Fachverband des
Tischlerhandwerks
Nordrhein-Westfalen

Wir gestalten Zukunft.
Gemeinsam.

EU-Datenschutz-Grundverordnung 2018

Das ändert sich 2018 beim Datenschutz
Die EU Datenschutzgrundverordnung (DSGVO) ersetzt zum 25.05.18 – nach einer zweijährigen Umsetzungsphase - viele nationale Datenschutzvorschriften, d.h. die DSGVO gilt unmittelbar. Ergänzend gilt das am 30.06.17 novellierte BDSG und tritt am gleichen Tag in Kraft. *(vgl. BGBl. I 2017, 2097ff)*

In die DSGVO sind viele Prinzipien der bisherigen Regelungen eingeflossen und ähneln den Vorschriften und der Dogmatik des Bundesdatenschutzgesetzes (BDSG). Die in der DSGVO niedergelegten Grundsätze unterscheiden sich daher praktisch nicht von den bisherigen Regelungen: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung oder Gewährleistung von Vertraulichkeit sind nicht neu.

Die DSGVO verstärkt die Betroffenenrechte und erhöht die Dokumentations- und Nachweispflichten, die zukünftig mit einem ausgeweiteten Bußgeldrahmen flankiert sind. Und glaubt man den Ankündigungen, werden die personellen Kapazitäten der Aufsichtsbehörden ausgebaut, damit dieser politisch gewollte effektive Datenschutz auch kontrolliert werden kann.

Die Neuerungen auf einen Blick:
- Die Definition personenbezogener Daten
- Einverständniserklärung erforderlich oder nicht?
- Neue Informations- und Dokumentationspflichten
- Datenschutz-Folgenabschätzung erforderlich?
- Datensicherheit
- Datenschutzbeauftragter
- Mögliche Strafen bei Verstößen
- Leitfaden zum Datenschutz

Die neuen Regeln betreffen alle, die personenbezogene Daten verarbeiten. Und das machen auch Verbände und Betriebe – weil sie Mitarbeiter beschäftigen, eine Kundendatenbank nutzen, Fotos von Referenzobjekten bei Facebook & Co. posten oder Mitarbeitern die private Nutzung von Firmenhandys erlauben.

Haus des Tischlerhandwerks

Kreuzstraße 108 - 110
44137 Dortmund

T + 49 (0) 231 – 912010 – 0
F + 49 (0) 231 – 912010 – 10
verband@tischler.nrw
www.tischler.nrw.de

Bankverbindung
Dortmunder Volksbank eG
BLZ 441 600 14
Kontonummer 2 301 038 301

Betroffene natürliche Personen müssen zukünftig umfassender darüber unterrichtet werden, warum welche Daten erhoben werden und die gesamte Datenerhebung muss zukünftig dokumentiert werden, um die Einhaltung der neuen Regeln gegenüber Behörden nachweisen zu können.

Bei der Umsetzung der neuen Regeln können Betriebe aber auch auf Muster zurückgreifen.

Wichtige Einschränkung:
Der Datenschutz umfasst ausschließlich natürliche Personen.
Daten juristischer Personen (z.B. staatliche Stellen, GmbH, AG, eingetragener Verein) werden nicht geschützt. *(vgl. Bundesbeauftragte für Datenschutz und Informationsfreiheit, Flyer „Datenschutz ist .., S.5, März 2017).*
Diese Einschränkung dürfte sich gerade bei Betrieben auswirken, deren Mitglieder / Kunden oft keine natürlichen Personen sind.

Die Definition personenbezogener Daten
Die EU-Verordnung (Art. 4 Abs. 1 DSGVO) definiert, was personenbezogene Daten sind. Sie berücksichtigt alles, wodurch sich Rückschlüsse auf eine Person ziehen lassen – also zum Beispiel
Name, Adresse, E-Mail-Adresse
Geburtsdatum, Bankdaten, Kfz-Kennzeichen, Fotos,
Cookies und IP Adressen

Grundsatz: Verbot mit Erlaubnisvorbehalt
Das sog. Verbot mit Erlaubnisvorbehalt (Art. 6, 7 DSGVO) wurde beibehalten, d.h. jede Datenverarbeitung – von der Erhebung über die Speicherung, Nutzung und Verwendung bis zur Weitergabe und Löschung – bedarf einer Rechtsgrundlage. Damit stellt sich die Frage:

Einverständniserklärung erforderlich oder nicht?
Bei der Verarbeitung von Kundendaten ist zwischen zwei verschiedenen Fällen zu unterscheiden.

Zulässig ist sie,
wenn sie für die Erfüllung eines Vertrages oder einer anderen gesetzlichen Verpflichtung erforderlich ist,
oder wenn die betroffene Person ausdrücklich in die Datennutzung eingewilligt hat.

Liegt eine gesetzliche Erlaubnis zur Datenverarbeitung vor, brauchen Betriebe keine gesonderte Einwilligung. Anders sieht es aus, wenn sie Kundendaten zu anderen Zwecken speichern wollen.
Zum Beispiel, weil sie Werbung per E-Mail versenden oder Telefon-Marketing betreiben wollen. Dann brauchen Betriebe die Einwilligung der Betroffenen, wie

es schon nach jetziger Rechtslage – insbesondere dem nicht datenschutzrechtlichen UWG *(Gesetz gegen den unlauteren Wettbewerb)* - der Fall ist.

Die Erlaubnis der Direktwerbung wird enger. Privilegien wie z.B. die Bewerbung von besonderen Aktionen, wie bisher in § 28 Abs. 3 BDSG geregelt, entfallen. Allerdings hilft hier bei der Auslegung der Erwägungsgrund 47 zur DSGVO, wonach die Verarbeitung personenbezogener Daten zum Zweck der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung angesehen werden kann.

Bestehende Einwilligungserklärungen sind weiter gültig. Die Einwilligung braucht nicht ausdrücklich „in Form einer Erklärung" abgegeben werden, eine konkludente „sonstige eindeutig bestätigende" Handlung reicht, so dass die Auftragserteilung, der Antrag auf Mitgliedschaft oder der Klick mit der Maus auch weiterhin die verbreitetste Form der Einwilligung bleibt.
Problematisch kann es künftig aber werden, wenn keine oder keine nachweisbare Einwilligung vorliegt. Für die Einwilligung wird zwar keine Schriftlichkeit gefordert, aber eine Nachweispflicht (Art. 7 DSGVO), die vor allem durch die „Schrift- oder Textform" ermöglicht wird.

Widerrufsrecht
Die betroffene Person erhält das Recht, die Einwilligung jederzeit zu widerrufen.

Informations- und Dokumentationspflichten *(Art. 13 DSGVO, §§ 32,33 BDSG neu)*
Betriebe haben neue Informationspflichten zu erfüllen. Personen, deren Daten verarbeitet werden, haben das Recht auf bestimmte Informationen.

- Namen und Kontaktdaten des für die Verarbeitung Verantwortlichen, d.h. des Verbandes oder Betriebes
- Zweck, für die die personenbezogenen Daten verarbeitet werden sollen
- Quelle der Daten
- Berechtigte Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
- Dauer, für die die personenbezogenen Daten gespeichert werden

Die Informationsrechte greifen auch immer dann, wenn sich Unternehmen von Betroffenen eine neue Einwilligungserklärung einholen. Denn dann müssen sie Kunden schriftlich darüber informieren, was sie mit den erhobenen Daten vorhaben – und zwar zum Zeitpunkt der Datenerhebung.

Auskunftsrecht
Betroffene bekommen zudem ein Auskunftsrecht. Auf Verlangen müssen Betriebe deshalb auch in einfachen Fällen künftig offenlegen, welche Daten sie von einer Person zu welchem Zweck gespeichert haben.

Verzeichnis für Verarbeitungstätigkeiten *(Art. 30 DSGVO)*

(bisher Verfahrensverzeichnis)

Neuerungen kommen insbesondere bei der Dokumentation auf Betriebe zu. So müssen sie künftig im sogenannten „**Verzeichnis für Verarbeitungstätigkeiten**" festhalten, welche personenbezogenen Daten im Unternehmen verarbeitet werden und wofür sie benutzt werden. Für Unternehmen unter 250 Beschäftigten gibt es hierzu Ausnahmen, sofern die Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, nur gelegentlich erfolgt oder keine besonderen Datenkategorien (Art. 9) oder Straftaten (Art. 10) einschließt.

Das dürfte nahezu bei allen KMU Betrieben – vor allem im Rahmen einer „normalen" Auftrag- und Vertragsabwicklung - der Fall sein.

In der Praxis können diese Ausnahmen allenfalls im Einzelfall dann nicht greifen, wenn sie z.B. bei einer internen Lohnbuchhaltung im Zusammenhang mit sensiblen Daten stehen (z.B. Gesundheitsdaten) Das Verzeichnis für Verarbeitungstätigkeiten soll dazu dienen, den Behörden Kontrollen zu erleichtern. Die Erstellung eines Verarbeitungsverzeichnisses „light" empfiehlt sich deshalb (siehe 2-seitiges ZDH Muster)

Recht auf Berichtigung, Löschen und Vergessenwerden

Betroffene Personen haben das Recht zu verlangen, dass unrichtige personenbezogene Daten unverzüglich berichtigt werden (Art. 16 DSGVO).

Zudem hat der Betroffene das Recht, jederzeit der Verarbeitung sie betreffender Daten und Profilings zu widersprechen. Dies gilt insbesondere, wenn diese für Werbung genutzt werden.

Eine wichtige Neuerung ist das Recht auf Löschung (Recht auf Vergessenwerden, Art. 17 DSGVO). Danach kann die betroffene Person verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, vor allem wenn die

- personenbezogenen Daten für den vorgesehenen Zweck nicht mehr notwendig sind
- die betreffende Person die Einwilligung widerrufen hat
- Löschung gesetzlich vorgeschrieben ist oder die personenbezogenen Daten unrechtmäßig verarbeitet wurden

Datenschutz-Folgenabschätzung erforderlich ?

Unter bestimmten Umständen muss die Dokumentation auch eine **Datenschutz-Folgenabschätzung** enthalten. Das ist nur dann der Fall, wenn ein hohes Risiko für die Rechte und Freiheiten der Betroffenen vorliegen kann. Als besonders sensibel gelten in diesem Zusammenhang Gesundheitsdaten, die ethnische Herkunft oder religiöse Zugehörigkeit einer Person. Solche Daten fallen in

Betrieben in der Regel aber nicht an, weshalb eine Datenschutz-Folgenabschätzung für den „normalen" Betrieb oft nicht relevant sein dürften.

Datensicherheit

Während bislang die Datenschutzgesetze einen Katalog von Maßnahmen vorgaben, indem sie technische und organisatorische Maßnahmen zur Datensicherheit forderten (z.B. Regelungen zum Zugriffsschutz, Schutz für die Weitergabe usw.), sind jetzt nur noch allgemeine Prinzipien vorgegeben. Es müssen aber nach wie vor geeignete technische oder organisatorische Maßnahmen getroffen werden, die sich am Stand der Technik orientieren.

Es ist also weiterhin erforderlich, dass eine Zugriffs- und Benutzerverwaltung existiert, die nur den dazu legitimierten Personen den Zugriff auf die Daten erlauben (z.B. Passwortvergaben)

Datenschutzbeauftragter

Voraussetzung der Bestellung eines – internen oder externen – Datenschutzbeauftragten ist, dass **„mindestens 10 (zehn) Personen ständig"** mit der Datenverarbeitung beschäftigt sind. Teilzeitbeschäftigte zählen dabei wie eine Person.

Bei der Empfehlung vieler IT Unternehmen, Datenschutzbeauftragte zu bestellen, sollte die Notwendigkeit aber im Einzelfall immer geprüft werden, nicht zuletzt wegen des Kündigungsschutzes des DSB (§§ 38, 6 BDSG)

Wichtig zur Berechnung des Schwellenwertes: „Ständig beschäftigt" ist, wer permanent Kunden- oder Personalverwaltung macht, nicht dagegen, wer z.B. als Handwerker oder Produktionsmitarbeiter nur mit Namen und Adressen von Kunden umgeht. (www.lda.bayern.de- datenschutzbeauftragter)

Neu ist die Pflicht nach Art. 37 Abs. 7 DSGVO, die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen (z.B. Webseite) und der Aufsichtsbehörde die Kontaktdaten zu melden. Um den Umstellungsaufwand bei der Bestellung eines neuen DSB möglichst gering zu halten, sollten allgemeine Kontaktadressen wie z.B. datenschutz@firma.de verwendet werden.

Mögliche Strafen bei Verstößen

Bei der rechtswidrigen Verarbeitung von personenbezogenen Daten können Unternehmen von der zuständigen Landesdatenschutzbehörde künftig mit einer Höchststrafe von bis zu 20 Millionen Euro oder 4 Prozent des gesamten weltweit erzielten Vorjahresumsatzes belangt werden, je nachdem welcher Betrag höher ist. § 43 BDSG neu regelt für Verstöße eine Geldbuße von bis zu 50.000,- €.
Mit diesen Höchststrafen werden Betriebe künftig sicher nicht belangt. Dennoch ist anzuraten, die neuen Regeln nicht auf die leichte Schulter zu nehmen.

Anhang: Datenschutz im Arbeitsrecht

Die Datenverarbeitung für Zwecke der Beschäftigungsverhältnisse wird in § 26 BDSG neu geregelt. Beschäftigtendaten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn

- sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit erforderlich ist und nicht anzunehmen ist, dass das schutzwürdige Interesse der betroffenen Person am Ausschluss der Verarbeitung überwiegt

- dies für die Begründung oder Durchführung eines Beschäftigungsverhältnisses oder der Erfüllung der sich aus Gesetz oder Tarifvertrag ergebenden Rechte und Pflichten erforderlich ist.

„Beschäftigte" ist ein weiter Begriff und bezieht sich nicht nur auf Mitarbeiter einschließlich Leiharbeitnehmer, sondern auch auf Auszubildende, Praktikanten und Heimarbeiter.
Die Einwilligung der Beschäftigtendaten muss freiwillig sein, d.h. für die Beschäftigten wird ein rechtlicher oder wirtschaftlicher Vorteil erreicht bzw. Arbeitgeber und Mitarbeitende verfolgen gleichgelagerte Interessen, was aber z.B. bei der Begründung eines Beschäftigungsverhältnisses eigentlich immer unterstellt werden kann.

Für die Einwilligung ist die Schriftform vorgeschrieben, wobei der Arbeitgeber die beschäftigte Person über den Zweck der Datenverarbeitung und das Widerrufsrecht in Textform aufzuklären hat, sinnvollerweise z.B. durch einen Passus im Arbeitsvertrag

Ausblick

Die Sach- und Rechtslage im neuen Datenschutz ist komplexer als bisher. Das bisherige deutsche Datenschutzrecht wird materiell zwar nur wenig geändert, aber zusätzlich geprägt durch ein komplizierteres Regelungsgeflecht. Bis der Umfang und die Geltung einzelner Bestimmungen für die Anwender rechtssicher bestimmt sind, wird noch einige Zeit vergehen
Wer aber zuvor nicht in die „Schusslinie tatendurstiger Datenschutzbehörden" geraten möchte sollte sich auf das neue europäische Datenschutzrecht einstellen, was aber m.E. keine „allzu große Herausforderung" darstellt. Insbesondere, weil u.a. der Leitfaden des ZDH dazu gute Vorgaben und Muster vorhält.

FACHVERBAND DES TISCHLERHANDWERKS NRW
RA Kemmerling