Neues zum Datenschutz

Die EU-Datenschutzgrundverordnung

Vortrag am 11.07.2018

Assessor Karl Fährmann
Datenschutzbeauftragter der
Handwerkskammer Aachen

Keine Panik!

1. Grundlagen

Keine Panik!

Die EU-Datenschutzgrundverordnung (EU-DSGVO)

➢ Was ist überhaupt die EU-Datenschutzgrundverordnung?

- Ein Rechtsakt der Europäischen Union
- Als Verordnung gilt dieser Rechtsakt unmittelbar in allen Mitgliedsstaaten der EU
- Es bedarf keines Umsetzungsaktes in nationales Recht
- Ergänzend gibt es weiterhin ein (neues) Bundesdatenschutzgesetz (BDSG neu)
- Es hat auch Anpassungen in Spezialgesetzen gegeben (z.B. HwO)
- Auch gibt es weiterhin Landesdatenschutzgesetze

Die EU-Datenschutzgrundverordnung (EU-DSGVO)

➢ Warum gibt es die EU-DGSVO?

- Die Vorgängerregelung auf europäischer Ebene, die Datenschutzrichtlinie (Richtlinie 95/46/EG), datiert aus dem Jahre 1995.
- Wenn man sich zurückerinnert, spielte damals das Internet praktisch noch keine Rolle, an Smartphones, Social-Media, Big-Data, Data-Mining, Scoring usw. dachte noch niemand.
- Regelung also nicht mehr zeitgemäß und kein unmittelbar geltendes Recht in den Mitgliedsstaaten.
- Der Datenschutz war (und ist) also europaweit sehr stark zersplittert. Problem dabei: Daten machen nicht an Grenzen halt.

Ab wann gilt die EU-DSGVO?

- Die EU-DSGVO gilt seit dem 25.05.2018!

- Aber es gibt doch bestimmt eine Übergangsfrist. Oder?

Nein, die EU-DSGVO gilt „scharf“ seit dem 25.05.2018. Sie wurde am 27.04.2016 verabschiedet, so dass wir uns jetzt nicht mehr in der „Übergangs-“ oder „Umstellungsfrist“ befinden.

- Aber die EU-DSGVO gilt doch dann bestimmt nur für neue Sachverhalte ab dem 25.05.2018. Oder?

Nein. Die EU-DSGVO gilt seit dem 25.05.2018 für sämtliche Sachverhalte, die den Datenschutz betreffen. Ob neue Sachverhalte oder solche aus dem Bestand, spielt keine Rolle. Allerdings bleiben z.B. erteilte Einwilligungen wirksam.

2. Regelungsgehalt

Was regelt denn die EU-DSGVO überhaupt?

- Die EU-DSGVO regelt den Umgang mit personenbezogenen Daten von natürlichen Personen (Art. 1 Abs. 1). Sie dient dem Schutz dieser Daten.

- Sie schützt somit die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2).

- Im deutschen Datenschutzrecht ist dies auch bekannt als das „Recht auf informationelle Selbstbestimmung“, welches seine Grundlage in Art. 1 und Art 2 des Grundgesetzes findet (Menschenwürde und allgemeine Handlungsfreiheit).

Was sind personenbezogene Daten?

- Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Personen angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Personen sind, identifiziert werden kann (Art. 4 Nr. 1).

- Unter Zuhilfenahme von technischen Möglichkeiten sind das de-facto alle Daten, die auch nur entfernt mit einer Person zusammenhängen!

Gilt das nur für externe Personen?

- Wie ist das denn bei Handwerksbetrieben? Wessen personenbezogene Daten werden denn dort verarbeitet?
  - Natürlich Kundendaten.
  - Auch Daten von Vertretern.
  - Und natürlich auch Mitarbeiterdaten!
- Was bedeutet „verarbeiten“? Jeder Umgang mit Daten, d.h. erheben, speichern, übermitteln, berichtigen, löschen, etc.

Was sind die Grundsätze der EU-DSGVO?

- Größtmögliche Transparenz für die betroffene Person, wenn ihre Daten verarbeitet werden.
- Das bedeutet umfangreiche Informationsansprüche, Auskunftsrechte, Rechte auf Berichtigung, Einschränkung der Verarbeitung, Löschung, Datenübertragbarkeit, ein Widerspruchsrecht, etc.
- Die betroffene Person soll weitestgehend Herrin ihrer Daten bleiben.
- Ein ganz wichtiger Grundsatz ist dabei ein Verbot mit Erlaubnisvorbehalt. Demnach ist erstmal jede Verarbeitung von personenbezogenen Daten verboten, wenn Sie nicht ausdrücklich erlaubt ist!

3. Datenverarbeitung

Wann ist eine Verarbeitung denn erlaubt?

Grundsätzlich gar nicht!

- Es sei denn, es gibt eine ausdrückliche Erlaubnis.

Mögliche Erlaubnistatbestände (Art. 6 Abs. 1):

- Einwilligung der betroffenen Person
- Zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist
- Zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt
- Zum Schutz lebenswichtiger Interessen der betroffenen Person
- Wenn die Verarbeitung erforderlich ist, zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt liegt, die dem Verantwortlichen übertragen wurde
- Wenn die Verarbeitung zur Wahrung berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen und Grundrechte (…) der betroffenen Person (…) überwiegen

Einwilligung

- Da die Einwilligung die in der Praxis wichtigste und auch flexibelste Form der Erlaubnis ist, sollen hier kurz die Anforderungen an eine wirksame Einwilligung dargelegt werden:

- Freiwillig
- Aktiv, d.h. keine vorangekreuzte Einwilligung zulässig
- Offenlegung der Identität des Verantwortlichen
- Angabe, welche Daten erhoben werden
- Angabe des Zwecks der Datenverarbeitung
- Hinweis auf Widerrufsrecht
- Optisch wahrnehmbar, d.h. abgesetzt von sonstigen Texten
- Textform ist nicht zwingend

Wer muss sich nun an die EU-DSGVO halten?

- Jeder Verantwortliche.
- Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (…) (Art. 4 Nr. 7).
- Also derjenige, der die personenbezogenen Daten verarbeitet (etwas verkürzt).
- Das gilt insofern natürlich auch für Handwerksbetriebe.

Pflichten des Verantwortlichen

- Welche Pflichten hat der Verantwortliche nach der EU-DSGVO ggü. der betroffenen Person?

- Bei der Datenerhebung muss der Verantwortliche die betroffene Person umfassend informieren
- Geschieht dies bei der betroffenen Person direkt (Art. 13), müssen folgende Informationen mitgeteilt werden:
  - Name und Kontaktdaten des Verantwortlichen
  - Ggfls. die Kontaktdaten des Datenschutzbeauftragten
  - Zwecke, für die die Daten verarbeitet werden sollen
  - Ggfls. die Empfänger oder Kategorien von Empfängern der Daten
  - Ggfls. die Absicht, Daten in Drittländer zu übermitteln
  - Dauer der Speicherung
  - Das Bestehen eines Rechts auf Auskunft, sowie auf Berichtigung, Löschung, Einschränkung der Verarbeitung
  - Hinweis, eine erteilte Einwilligung jederzeit widerrufen zu können
  - Das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde
  - Ob die Bereitstellung der Daten verpflichtend ist und welche Folgen bei Nichtbereitstellung drohen

Pflichten des Verantwortlichen

- Wann und in welcher Form muss die betroffene Person nach Art. 13 EU-DSGVO bei der Datenerhebung informiert werden?
- Die Informationen müssen „zum Zeitpunkt“ der Datenerhebung mitgeteilt werden.
- Bei einem schriftlichen Vertragsabschluss oder einem längeren Beratungsgespräch in einem Ladenlokal (z.B. Gesundheitshandwerke) ist dies in der Regel über ein Beiblatt o.ä. unproblematisch möglich.
- Ansonsten wäre auch ein Aushang im Lokal und, wenn vom Kunden gewünscht, die Aushändigung eines Abdrucks denkbar.
- Bei Bestellungen im Internet ist die Einbindung der Information in den Registrierungs- bzw. Bestellvorgang unproblematisch möglich.
- Bei telefonischen Bestellungen könnte eine SMS auf Handy die notwendige Information gewährleisten, ansonsten ein Hinweis auf eine leicht zu merkende Internetseite.
- Hinsichtlich der Beschäftigten im Unternehmen ist eine Informationsseite im betrieblichen Intranet ein sinnvoller Informationswert.

Welche Rechte bzw. Ansprüche hat die betroffene Person?

- Welche Ansprüche und Recht hat eine betroffene Person nach der EU-DSGVO?
- Auskunftsrecht (Art. 15)
- Recht auf Berichtigung (Art. 16)
- Recht auf Löschung (Art. 17). Wird auch „Recht auf Vergessenwerden“ genannt, da der Verantwortliche nicht nur die bei ihm gespeicherten Daten löschen muss, sondern u.U. auch dafür Sorge tragen muss, dass auch andere Verantwortliche entsprechende Links, Kopien etc. dieser Daten zu löschen hat.
- Recht auf Einschränkung der Verarbeitung (Art. 18)
- Recht auf Mitteilung (Art. 19)
- Recht auf Datenübertragbarkeit (Art. 20)
- Widerspruchsrecht (Art. 21)
- Recht, eine erteilte Einwilligung jederzeit zu widerrufen (Art. 7, Abs. 3)

4. Konkrete Umsetzung

Was muss denn nun genau gemacht werden?

- In formeller Hinsicht:
  - Muss ein Datenschutzbeauftragter benannt werden?
  - Muss ein Verzeichnis der Verarbeitungstätigkeiten angelegt werden?
  - Müssen technisch-organisatorische Maßnahmen ergriffen und dokumentiert werden?
  - Muss das Vorgehen im Datenschutz dokumentiert werden?
  - Anpassung der Datenschutzerklärung auf der Homepage?

- In materieller Hinsicht:
  - Überprüfung von Einwilligungserklärungen auf Konformität mit EU-DSGVO
  - Überprüfung von sonstigen Unterlagen auf Konformität mit EU-DSGVO
  - Überprüfung, ob die Verträge mit den Auftragsdatenverarbeitern der EU-DSGVO entsprechen
  - Überprüfung, ob eine Datenübermittlung in Drittstaaten, d.h. das Nicht-EU-Ausland erfolgt

Datenschutzbeauftragter?

- Wann muss ich in meinem Unternehmen einen Datenschutzbeauftragten benennen?

- Dies richtet sich nach Art. 37 Abs. 4 nach § 38 BDSG neu.

- Ein DSB muss dann benannt werden, wenn im Betrieb in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung von Daten beschäftigt sind.

- Wie der Begriff „ständig“ auszulegen ist, ist umstritten. Zumindest nach Ansicht des Bayerischen Landesamtes für Datenschutzaufsicht soll es sich dabei um eine Haupttätigkeit der jeweiligen Person handeln.

- Bei vielen Handwerksbetrieben wird also diese Anzahl von Mitarbeitern nicht überschritten werden.

Datenschutzbeauftragter?

➢ Gesundheitshandwerke

- Eine besondere Fallgruppe bilden die Gesundheitshandwerke.
- Darunter fallen Augenoptiker, Hörakustiker, Orthopädietechniker, Orthopädieschuhmacher und Zahntechniker.
- Diese verarbeiten Gesundheitsdaten und damit besonders sensible Daten nach Art. 9 EU-DSGVO.
- Ob diese Betriebe deswegen grundsätzlich einen DSB beauftragen müssen, ist streitig, zumindest das bayerische Landesamt für Datenschutzaufsicht geht davon aus. Der LDI NRW stellt auf eine Einzelfallbetrachtung ab (siehe auch nächste Folie).

Datenschutzbeauftragter?

➢ Fotografenhandwerk

- Ein weitere Sonderfall sind Fotografen, die schwerpunktmäßig biometrische Passbilder erstellen.
- Auch biometrische Daten sind besonders sensible Daten nach Art. 9 EU-DSGVO.
- Hier stellt sich, ebenso wie bei den Gesundheitshandwerken, die Frage, ob deswegen grundsätzlich ein DSB zu benennen ist.
- Nach Einschätzung des LDI NRW ist darauf abzustellen, ob hier in umfangreicher Form solche Daten verarbeitet werden. Bei einem Fotografenbetrieb „normaler“ Größe wird dies eher nicht der Fall sein, so dass dann kein DSB zu benennen wäre.

Kleiner Einschub: Fotografieren

- Als besonders heikel i.S.d. EU-DSGVO wird in der Öffentlichkeit das Fotografieren dargestellt

- Das Fotografieren stellt, wenn Personen fotografiert werden, natürlich ein Verarbeiten von personenbezogenen Daten dar.

- Es gelten aber die allgemeinen Erlaubnistatbestände der EU-DSGVO auch hier, d.h. Einwilligung, Erfüllung eines Vertrages, überwiegendes Interesse.

- Auch hier gelten die allgemeinen Informationspflichten nach Art. 13 EU-DSGVO.

- Das Kunsturhebergesetz (KUG), das die Veröffentlichung von Bildern regelt, gilt weiterhin.

Datenschutzbeauftragter?

➢ Schornsteinfeger

- Eine weitere Besonderheit besteht im Schornsteinfegerhandwerk.
- Ist der Schornsteinfeger auch bevollmächtigter Bezirksschornsteinfeger, muss ein DSB bestellt werden.
- Der bevollmächtigte Bezirksschornsteinfeger gilt nämlich als öffentliche Stelle nach § 2 Abs. 4 Satz 2 BDSG-neu, da hoheitliche Aufgaben der öffentlichen Verwaltung wahrgenommen werden.

Verzeichnis der Verarbeitungstätigkeiten?

- Muss ich in meinem Betrieb ein Verzeichnis der Verarbeitungstätigkeiten (VV) führen? Und was ist das?
  - Das VV ist eine Übersicht, über die im Unternehmen bestehenden, datenschutzrechtlichen Verfahren. Geregelt in Art. 30.
  - Im VV ist u.a. aufzuführen, welche Daten wozu, wie lange, auf welcher Rechtsgrundlage verarbeitet werden und ob Übermittlungen in Drittstaaten erfolgen.
  - Ein VV muss von jedem Verantwortlichen geführt werden, es sei denn, es greift die Ausnahme aus Art. 30 Abs. 5.
  - Diese ist aber eng auszulegen und es ist auch sehr sinnvoll, ein VV zu führen. Allein um zu erkennen, wo überhaupt personenbezogene Daten verarbeitet werden.
  - Beispiele: Personaldatenverwaltung, Kundendatenbank, Videoüberwachung, etc.

Technisch-Organisatorische Maßnahmen (TOM)

➢ Was sind TOM?

- Die Maßnahmen, die unter Berücksichtigung von acht Kriterien ein dem Risiko angemessenes Schutzniveau gewährleisten (Ehmann/Selmayr, Datenschutzgrundverordnung, Art. 32, Rn. 4).

- Kriterien sind: Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zweck der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

- Beispiele: Wie sind Zugänge zu den PCs geschützt, Schutz des Serverraums, Zugangskontrolle zum Gebäude, werden Datenschutztonnen für Papier verwendet, wird die IP-Adresse des Nutzers der Homepage gespeichert, gibt es eine Videoüberwachung, gibt es Alarmanlagen, gibt es eine Firewall, etc

5. Verstöße

Was passiert bei Verstößen gegen die EU-DSGVO?

- Was kann bei Verstößen gegen die Regelungen der EU-DSGVO passieren?

- Die EU-DSGVO sieht sehr unangenehme Bußgelder bei Datenschutzverstößen vor.
- Es sind Bußgelder in Höhe von bis zu 20.000.000 € oder bis zu 4 % des gesamten, weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres möglich, je nachdem, welcher der Beträge höher ist.
- Alphabet Inc., die Muttergesellschaft von Google, hatte 2017 einen Jahresumsatz von 110.800.000.000 US $.
- Das maximale Bußgeld betrüge somit gute 4 Milliarden US $!
- Die EU-DSGVO sieht in Art. 82 auch Schadenersatzansprüche der betroffenen Person vor.
- Es sind ferner Klagen nach dem Unterlassungsklagengesetz (UKlaG) denkbar (§ 2 Abs. 2 Satz 1 Nr. 11 a, b UKlaG)
- Auch Abmahnungen durch Konkurrenten oder betroffene Personen sind denkbar.

Bewertung/Empfehlungen

- Kann man denn schon eine Bewertung zur EU-DSGVO abgeben bzw. kann man Empfehlungen aussprechen?

- Vieles ist von der Struktur her schon jetzt geltendes Recht, einige Neuerungen gibt es aber.
- Es kommt auf Betreibe und Behörden ein nicht unerheblicher Umstellungsaufwand zu .
- Das Bewusstsein der betroffenen Personen und Verkehrskreise für das Thema Datenschutz wird deutlich geschärft werden.
- Man sollte die Einführung der EU-DSGVO aber auch als Chance begreifen.
- Durchleuchten Sie, an welchen Stellen im Betrieb überhaupt personenbezogene Daten verarbeitet werden.
- Ändern und verbessern Sie ggfls. Verfahren.
- Treten Sie offensiv mit einem hohen Datenschutzniveau auf.

Muster/Hilfen/Leitfaden

- Der ZDH hat sehr umfangreiche Materialien für Handwerksbetriebe zur Umsetzung der EU-DSGVO entwickelt.
- Diese sind auf den Homepages Ihrer jeweilige Handwerkskammern abrufbar (ansonsten auf www.hwk-aachen.de).
- Sie finden dort einen Leitfaden zur Umsetzung, Musterformulare und Kurz-Informationen im Format „ZDH-Praxis-Datenschutz“.


Fragen?

Handwerkskammer Aachen
Sandkaulbach 17 – 21
52062 Aachen

Telefon: 0241-471-141
karl.faehrmann@hwk-aachen.de

www.hwk-aachen.de