EU-Datenschutz-Grundverordnung (EU-DSGVO) 25.05.2018

Allgemein

Die EU-Datenschutzgrundverordnung gilt unmittelbar in allen EU-Mitgliedstaaten ab dem 25. Mai 2018.
Somit wird auch die Übergangsregelung zur Anpassung des BDSG vom 05.07.2017 überholt sein.
Daher beschäftigen wir uns in der Folge ausschließlich mit der neuen VERORDNUNG.

Die EU möchte mit dieser Grundverordnung, neben dem individuelleren Schutz von Privatpersonen, gleichwohl den Aspekt der Datenflut regeln. Motto: Weniger ist mehr… so widergespiegelt im Art. 5 Abs. 1c DSGVO.

Systematik

Die Grundprinzipien des neuen Datenschutzrechtes sind:

- Rechtmäßigkeitsgrundsatz (Rechtsgrundlage)… hier genügt die reine Einwilligung nicht mehr!
- Zweckbindungsgrundsatz (Erforderlichkeit)
- Verhältnismäßigkeitsgrundsatz (Datenminimierung)
- Grundsatz der Richtigkeit aller Daten
- Grundsatz der Transparenz (Info, Auskunft, Benachrichtigung)… binnen eines Monats muss die Anfrage der Datenschutzbehörde seitens des Betroffenen erl. sein
- Grundsatz der Datensicherheit und Vertraulichkeit der Daten… wenn bspw. PC verloren geht (gestohlen wurde) müssen alle Personen, die auf der Festplatte / outlook, etc. gespeichert wurden, somit informiert werden und gleichfalls auch die Datenschutzbehörde

… bei Nichtbeachtung relevanter Artikel werden neben Bußgelder auch „Schmerzensgelder“ aufgerufen von Personen, die plötzlich sagen, „… dass die Persönlichkeitsrechte, etc. verletzt wurden durch den Datenverlust….“.

Dieses Thema des Schmerzensgeld wird stark aufkommen, da keinerlei Einwilligung bspw. gegeben ist, ein Foto von Jemanden gemacht zu haben und auf facebook abzulichten oder bei einer Wohnungsbegehung wenn eine Flasche Sprudel mit gefilmt wird und somit das Trinkverhalten der betroffenen Person ersehen werden kann (denn die bisherigen Einwilligungen sind nicht mehr konform dem Text nach, was nun abverlangt wird i.R. d DSGVO!)

Hierbei stellt sich gleichwohl für jeden Verantwortlichen / Anwender die Frage nach der **Ausweitung der Betriebs-HV**! Erfahrungsgemäß haben die Versicherer hier keinen „Plan“.

Sachlicher Anwendungsbereich (nichtöffentl. Stellen –Firmen, etc.-)

Ganz oder teilw. automatisierte Verarbeitung personenbezogener Daten
oder
Nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder werden sollen.

(Ausnahme: Ahnenforschung = keine Anwendung der Datenschutzgrund-verordnung)

Räumlicher Anwendungsbereich

- Inland
- Ausland aber für inländische Niederlassungen
- oder Auftragsverarbeiter Datenverarbeitung erfolgt außerhalb EU/EWG, betrifft aber Personen der EU.

Checkliste zur Anwendbarkeit DSGVO

Verarbeiter	→ Werden Dienstleistungen/Waren in D angeboten? → Werden Dienstleistungen/Waren in der EU angeboten? → Haben Sie Mitarbeiter in Ihrem Unternehmen

Auftragsverarbeiter	→ Werden Dienstleistungen/Waren in Deutschland im Auftrag eines Dritten angeboten? → Werden Dienstleistungen/Waren in der EUR im Auftrag eines Dritten angeboten?

Wenn nur eine Frage mit **JA** beantwortet wird, sind Sie Verarbeiter oder Auftragsverarbeiter und es gilt die neue DSGVO!

<u>Begrifflichkeiten</u>

Personenbezogene Daten
=
Alle Informationen, die sich auf eine identifizierte natürliche Person (betroffene Person) beziehen (gespeicherte Handynummer im Handy, whats app, etc.)
… als indentifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer online-Kennung oder weiteren Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser betroffenen Person sind!

Verarbeitung
=
Jeder Vorgang im Zusammenhang mit personenbezogenen Daten mit oder ohne Hilfe automatisierter Verfahren ausgeführt, wie bspw. Erheben, Erfassen, die Organisation, das Ordnen (also bereits ein wilder Stapel auf dem Büroboden), die Speicherung, die Anpassung der Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung der Daten.

Automatisierte und nicht automatisierte Verfahren
=
Die DSGVO bezieht jede automatisierte Verarbeitung und nichtautomatisierte Verarbeitung bei Speicherung in ein Dateisystem ein. Eine automatisierte

Verarbeitung liegt bei der Benutzung von Computer, smartphones, Kameras, Webcams, Dashcams, scanner oder Kopierer vor, wenn personenbezogene

Daten betroffen sind. Eine nichtautomatisierte Verarbeitung liegt insb. bei handschriftlichen Aufzeichnungen vor.

Dateisystem
=
Jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet und soweit geführt wird (also auch Ordner).

Verantwortlicher
=
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; sind die Zwecke und Mittel dieser Verarbeitung durch Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

Verantwortlicher ist der GF (nicht der Datenschutzbeauftragte!)

Bereits ab 10 aktiv zu einem Betrieb gehörende Funktionsträger (auch freie Mitarbeiter, beauftragter Hausmeister bei einer WEG, etc.) muss ein Datenschutzbeauftragter bestellt werden. Bei einem Verein mit 10 unterschiedlichen Funktionsträger (also schon 10 individuelle Email-accounts), was schnell erreicht ist, ist ein Datenschutzbeauftragter zu bestellen!

Aus der Praxis

Datenerhebung bei einer Mietvertragsanbahnung (dieses Szenario wird gewählt, da relevant für Kunden der VSK):

Makler/Verwalter/Vermieter annonciert im Internet eine freie Wohnung zum Vermieten. Es melden sich viele Interessenten.

Welche Daten hätte der Vermieter gerne? Und welche Daten dürfen tats. erhoben und verarbeitet werden?

Exkurs
Früher hatte eine Einwilligung genügt, um den Mietinteressenten abzufragen bzw. ihm dann eine Selbstauskunft hinter her zu schieben. Da die Einwilligung nunmehr so eine große Hürde darstellt ob des sprachlichen Verständnisses, dem sprachlichen Duktus, etc. besitzt, ist von einer Einwilligung als Grundlage des Auskunftsbegehrs abzuraten. Auch mangelt es an der Freiwilligkeit, denn der Mietinteressent ist angewiesen Infos zu liefern, sonst gibt es keine Wohnung; daher liegt keine Freiwilligkeit vor. Die Brücke/Lösung ist somit = berechtigtes Interesse.

Somit sind vor jeder Datenerhebung deshalb der Zweck zu ermitteln und danach erst der Umfang der Datenerhebung zu bestimmen. Im Rahmen der Vertragsanbahnung zum Mietvertrag ist in unterschiedlichen Phasen zu unterscheiden.

Lösungsansatz bei der Suche des geeigneten Mieters

Welche Daten sind für die Auswahlentscheidung relevant?

- Bonitätsprüfung
- Bisheriges Wohnverhalten
- Beabsichtigte Nutzung (Tiere, Gewerbe…)
- Stabile Bewohnerstruktur
- Ausgeglichene soziale und kulturelle Verhältnisse

…o.g. Paramater sind zu erhalten bspw. durch

- Selbstauskunft, Ausweiskopie
- VSK-Mietercheck
- Nachfrage Vorvermieter

Und somit wieder = Keine Datenverarbeitung (Erfragung) ohne Rechts-grundlage!

Mögliche Ansätze der Rechtsgrundlagen
=
1) Einwilligung
2) Vertragserfüllung
3) Berechtigte Interesse
4) Rechtspflicht

Kurz mit einem Beispiel unterlegt =
Ein Geburtsdatum wäre zunächst Pflichtangabe seitens eines Mietinteressenten. Die Lösung kann hierzu sein, im Mietvertrag das Geb.datum mit aufzunehmen. Somit wäre das Geb.datum für eine bspw. spätere Adressermittlung, weil Miete aussteht, doch noch im Archiv und nicht von der sofortigen betroffen, da nämlich das Geb.datum nicht gespeichert werden dürfte für Belange der Selbstauskunft.

Zusammenfassung zum Thema Rechtsgrundlage
=
1) Einwilligung = Von dieser Rechtsgrundlage ist abzuraten
2) Vertragserfüllung = auch ohne Einwilligung ist diese Überlegung rechtmäßig (Art. 6 Abs. 1b DSGVO)
3) Die HAUPT-BRÜCKE zur Lösung = es bestehen tatsächliche oder rechtliche Beziehungen zwischen der verantwortlichen Stelle und der betroffenen Person oder diese sollen angebahnt werden und das vernünftige Interesse der betroffenen Person überwiegt nicht!
   ↓ **Bsp.**
   - Daten im Rahmen von Kundenbeziehungen reichen aus
   - Daten von Anbieter bestimmter Dienstleistungen/Waren
   - Daten über Suchverhalten im Internet (google !)
   - Auswertung von Bestandsdaten im Rahmen von Mietverhältnissen

Und schauen sie mal… (Erweiterter Gedanke)
=
Allg. Gleichbehandlungsgesetz (AGG)
↓

Bei der Vermietung von Wohnraum ist eine unterschiedliche Behandlung im Hinblick auf die Schaffung und Erhaltung sozial stabiler Bewohnungsstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse zulässig!

D.h. alles kann erfragt werden bspw. im Rahmen der Selbstauskunftsbefragung, allerdings nicht gespeichert! Darauf kann man dann trotzdem seine Entscheidung treffen.

Weitere Begriffe und Überleitung zu notwendigen Verträgen, etc.

Verantwortlicher
Verantwortlicher i.S. der DSGVO ist die Geschäftsleitung. Dieser erhebt aber ja nicht immer selbst die Daten, sondern lässt die Daten durch seine Mitarbeiter oder durch Dritte unmittelbar erheben (sog. Auftragsverarbeiter).

Auftragsverarbeiter
Natürliche oder juristische Personen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Die wesentlichen Vorgaben zur Auftragsverarbeitung sind in Art. 28 geregelt. Deswegen wird hier meinerseits empfohlen mit einem AUFTRAGSVERARBEITUNGSVETRAG zu operieren. Ob bei der VSK mit Kunden, einer Objekt-GmbH mit Handwerker, etc. überall sind Daten im Austausch, der Archivierung und Nutzung dieser. So schützt ein Auftragsverarbeitungsvertrag den Verantwortlichen schon i.S. der Beachtung der neuen DSGVO. Vor allem betr. des rasch aufgerufenen Schmerzensgeld-Thematik, wonach sicher Armadas von „fast arbeitslosen“ Anwälten Abmahnungen zahlreich versenden werden.

MUSTER

Und, … der Verantwortliche muss gleichwohl ein VERARBEITUNGSVERZEICHNIS nach Art. 30 As. 2 DSGVO führen. Dies muss auch der Auftragsverarbeiter selbst ebenfalls erstellen (dies wissen diese derzeit aber noch nicht).

MUSTER

Denn im Falle der Beauftragung eines Dritten mit der Verarbeitung personenbezogener Daten (Auftragsverarbeitung) ist der Verantwortliche des Auftraggebers für die Einhaltung aller Datenschutz-Bestimmungen zuständig.

Die Auftragsverarbeiter wiederum dürfen ohne schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen.
Zwischen Verantwortlichen und Auftragsverarbeiter ist zwingend ein schriftlicher oder elektronischer Vertrag abzuschließen.
↓
Darin sind inhaltliche MUSTS zu berücksichtigen
=
Dauer, Art und Zweck der Verarbeitung, Weisung des Verantwortlichen, Einhaltung bestimmter Rechte der betroffenen Person, Sicherheit der Datenverarbeitung, etc.

Informationspflicht bei der Datenerhebung Art 13, 14 DSGVO

=
Der Verantwortliche hat der betroffenen Person zum Zeitpunkt der Erhebung personenbezogener Daten folgendes mitzuteilen:

- Name und Kontaktdaten des Verantwortlichen und ggfl. der Datenschutz-beauftragten
- Zweck der Datenverarbeitung und Rechtsgrundlage sowie Dauer der Speicherung
- Gggfl. Empfänger oder Kategorie von Empfängern der personenbezogenen Daten
- Hinweis auf Auskunftsrecht, Beschwerderecht, Widerrufsrecht, Recht auf Löschung usw.
- Zusätzlich auch die Kategoeire personenbezogener Daten, die verarbeitet werden, wenn die Datenerhebung nicht bei der betroffenen Person erfolgt

Beispielsweise auf die Spitze getrieben = Anzuwenden eigentlich auch bei vom Handwerker auf dessen Handy gespeicherten Vermieter-/Kunden-Daten, im outlook gespeicherten Email-Adressen (dropdown dort), etc.

MUSTER

Rechtsfolge von Verstößen gegen das DSGVO

=

1) Verletzung des Schutzes personenbezogener Daten
   → Benachrichtigungspflicht der betroffenen Person Art. 34 DSGVO
2) Schadensersatz und Sanktionen
   → Schadensersatz (Art. 82 DSGVO)… gibt noch keine Erfahrungswerte; kann aber schon je Einzelfall mit EUR 200 – 2.000 aus akt. Sicht zu beachten sein.
   → Geldbußen gem. Art. 83 DSGVO… bis zu TEUR 50 bei Kleinunternehmen
3) Umgang mit der Aufsichtsbehörde
   → Meldepflicht (Art. 33 DSGVO)

Checkliste zur Einhaltung/Vorbereitung zur neuen DSGVO

Schritt 1 Vorbereitung

1) Geschäftsleitung ergreift Initiative zur Umsetzung des Datenschutzes (= Verantwortlicher)
2) GS bestimmt Zuständigkeiten und verteilt die anstehenden Aufgaben
3) GS ermittelt und bestimmt ggfl. einen Datenschutzbeauftragten
4) GS lässt Bestandsaufnahme durchführen und ein Verzeichnis aller Verarbeitungstätigkeiten erstellen

Schritt 2 Umsetzung

1) Ermittlung der Rechtsgrundlagen der Datenverarbeitung
2) Prüfung, ob Einwilligungen der betroffenen Personen erforderlich sind und Überprüfung, ob rechtswirksame Einwilligungen vorliegen (hier mein Kommentar auf Umgehung beachten!!!!)
3) Prüfung, ob Auftragsverarbeiter eingeschaltet sind und ob wirksame Verträge mit diesen geschlossen sind
4) Prüfung, ob und wie Informationspflicht, Auskunftsrecht, Recht auf Berichtigung, Recht auf Löschung, Recht auf Datenübertragbarkeit, Widerspruchsrecht der betroffenen Personen erfüllt werden
5) Prüfung, ob Datenschutz durch Technikgestaltung und Voreinstellungen gewährleistet ist sowie Datensicherheit (Passwort bspw. bei outlook und PC –Zugang…)
6) Festlegung, was und von wem im Falle von Datenschutzverletzungen zu tun ist

Schritt 3 Wiederkehrende Aufgaben

1) Sicherstellung, dass der Verantwortliche regelmäßig über Änderungen in betrieblichen Abläufen, die die Verarbeitung personenbezogener Daten betreffen, informiert wird
2) Sicherstellung, dass Änderungen in betrieblichen Abläufen, die die Verarbeitung personenbezogener Daten betreffen, dokumentiert werden
3) Sicherstellung, dass Mitarbeiter in regelmäßigen Abständen über datenschutzrechtliche Rechte und Pflichten informiert und geschult werden.

ARU, Stuttgart im März 2018