DSGVO kompakt:
Was sie jetzt wissen müssen

Anwaltverein Dortmund, 02.05.2018

Christian Oberwetter
Fachanwalt für Arbeitsrecht
und IT-Recht
Hamburg/Berlin

Das Seminar im Überblick

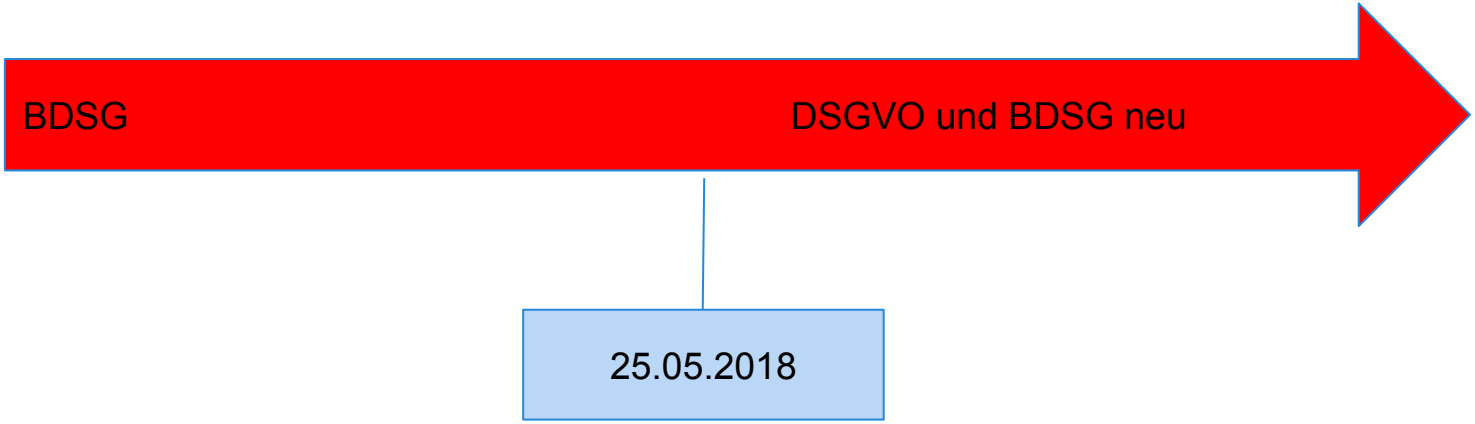
1. Grundlegendes zur Neuregelung

2. Datenverarbeitung in der Anwaltskanzlei, Informationspflichten und Betroffenenrechte, Datensicherheit

3. Datenschutz und Mitarbeiter

Grundlegendes zur Neuregelung

Überblick: Derzeitige und künftige Rechtslage



Geltungsbereich/ Definitionen

Ziel der DS-GVO ist es

- eine EU-weite Einheitlichkeit erreichen
- den Datenschutz zu modernisieren
- gleiche wirtschaftliche Bedingungen in allen EU-Staaten zu schaffen

Daher **Verordnung** und nicht Richtlinie (wie Richtlinie 95/46/EG)

entgegenstehendes nationales Recht ist aufzuheben

Öffnungsklauseln für einzelne Bereiche vorgesehen

daher BDSG-neu

Geltungsbereich/Definitionen

Struktur der DS-GVO

- 99 Artikel

Ähnlich Paragraphen in Gesetzen

- 173 Erwägungsgsgründe

Die Erwägungsgründe sind eine Gesetzesbegründung.

Sie sind wichtig zur Auslegung des Verordnungstextes

Auch wenn Erwägungsgründe ‚nur' nach Erläuterungen klingt, sind diese ebenso verbindlich wie die Festlegungen in den Artikeln

Ermöglichen in vielen Fällen ein erweitertes Verständnis der zugeordneten Artikel

Geltungsbereich/ Definitionen

Praxisfrage: Wie zurechtfinden?

- Als EU-Verordnung hat die DS-GVO Anwendungsvorrang vor dem BDSG-neu
- deshalb Orientierung grundsätzlich an DS-GVO, aber in bestimmten Bereichen (z.B. Beschäftigtendatenschutz) schafft BDSG spezifischere Regeln
- Orientierung auch an Umsetzungshilfen und Kommentaren der Aufsichtsbehörden

Beispiel: Bayerisches LDA

Geltungsbereich/Definitionen

- **personenbezogene Daten, Art. 4 Nr. 1 DS-GVO**
- **Verarbeitung, Art. 4 Nr. 2 DS-GVO**
- **Verantwortlicher, Art.4 Nr.7 DS-GVO**

- 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 (…).“

also hier: die Anwaltskanzlei

- **Auftragsverarbeiter, Art. 4 Nr.8 DS-GVO**

- eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

also: Dienstleister, der für Anwaltskanzlei personenbezogene Daten verarbeitet

Was ist zu tun? Verarbeitung in der Anwaltskanzlei

© Niki Love - Fotolia.com #79892602

Was ist zu tun?
Verarbeitung in der Anwaltskanzlei

1. Benötigt die Kanzlei einen Datenschutzbeauftragten?
2. Muss ein Verarbeitungsverzeichnis geführt werden und was ist zu beachten?
3. Welche Informationspflichten gelten und was ist mit den Betroffenenrechten?
4. Welche Maßnahmen zur Datensicherheit muss ich treffen? Darf nur noch per verschlüsselter E-Mail mit Mandanten kommuniziert werden?

Der Datenschutzbeauftragte

Ein Datenschutzbeauftragter (DSB) muss nach Art 37 Abs.1 DSGVO bestellt werden, wenn

- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen,
- die Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht

oder nach § 38 BDSG, wenn

- in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind

Der Datenschutzbeauftragte

Liegt die Kerntätigkeit in der umfangreichen Verarbeitung (besonderer) personenbezogener Daten?

- Kerntätigkeit des Anwalts ist es, Rechtsdienstleistungen zu erbringen (§ 2 I RDG). Das geht regelmäßig mit der Verarbeitung personenbezogener Daten einher
- Ob die Verarbeitung umfangreich ist, ist im Einzelfall zu entscheiden
- Insbesondere strafrechtlich ausgerichtete Kollegen können zukünftig zur Bestellung eines Datenschutzbeauftragten nach Art. 37 I Buchst. c DS-GVO verpflichtet sein

Verarbeiten zehn oder mehr Personen ständig in der Kanzlei pbD?

- hierzu zählen Anwälte, RA-Fachangestellte, Referendare, studentische Aushilfen etc.

Der Datenschutzbeauftragte

- nur noch von einer „Benennung“ des DSB die Rede, d.h. keine schriftliche Bestellung mehr
- Verantwortlicher veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt die Daten der Aufsichtsbehörde mit, Art.37 Abs.7 DSGVO
- Auch weiterhin ein externer DSB möglich (Art. 37 Abs. 6 DSGVO)
- Anforderungen nach Art. 37 Abs. 5 DSGVO:
  - eine gewisse berufliche Qualifikation,
  - das Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis und
  - die Fähigkeiten zur Erfüllung der gesetzlich definierten Aufgaben

Interessenkonflikte sind zu vermeiden (Art. 38 Abs. 6 DSGVO)

Der Datenschutzbeauftragte

Aufgaben, Art 39 DSGVO

- Unterrichtung und Beratung der Verantwortlichen, der Auftragsverarbeiter und der Beschäftigten
- Überwachung der Einhaltung der DSGVO und nationalen Sonderregelungen
- Sensibilisierung und Schulung
- Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde

vertiefend: Kazemi, Der Datenschutzbeauftragte in der Rechtsanwaltskanzlei, NJW 2018, 443

Rechtmäßigkeit der Verarbeitung

Art. 5 DSGVO in Kurzform

Ich darf pbD nur

- auf rechtmäßige, transparente Weise
- für eindeutig festgelegte Zwecke verarbeiten
- dabei nur so viele Daten erheben wie notwendig
- muss darauf achten, dass es sich um korrekte Daten handelt
- und ein Rückschluss auf Personen darf nur bis zur Erreichung der Zweckerfüllung möglich sein
- und schließlich muss ich die pbD vor Zugriffen von außen schützen (TOM)

Rechtmäßigkeit der Verarbeitung

Art. 6 DSGVO - Wann darf ich verarbeiten?

- Einwilligung (lit.a)
- zur Vertragserfüllung erforderlich (lit.b)
- zur Erfüllung einer rechtlichen Verpflichtung (lit c.)
- zum Schutz lebenswichtiger Interessen (lit. d)
- öffentliches Interesse (lit. e)
- berechtigtes Interesse (lit.f)

Es gilt weiterhin: Grundsatz des Verbots mit Erlaubnisvorbehalt!

Rechtmäßigkeit der Verarbeitung

Die Einwilligung

Form:

EG 32 DSGVO: auch elektronische oder mündliche Form zulässig, aber

- Art. 7 Abs.1 DSGVO: Verantwortlicher muss Nachweis führen, dass Einwilligung erteilt wurde
- Art. 7 Abs.2 DSGVO: Einwilligung muss verständlich, leicht zugänglich in klarer einfacher Sprache, klar unterscheidbar von anderen Erklärungen sein
- siehe speziell § 26 BDSG

Freiwilligkeit:

- EG 43 DS-GVO: fehlt, wenn klares Ungleichgewicht zwischen Betroffenen und Verantwortlichen (siehe auch § 26 BDSG)
- Art. 7 Abs.4 DS-GVO: fehlt, wenn Einwilligung für die Erfüllung des Vertrages nicht notwendig (Koppelungsverbot)

Rechtmäßigkeit der Verarbeitung

Grundsatz der informierten Einwilligung
Aufklärung über:

- die Identität des für die Verarbeitung Verantwortlichen
- den Zweck (und den Umfang) jeder Verarbeitung, für die eine Einwilligung verlangt wird;
- welche Art von Daten gesammelt und verwendet werden
- das Bestehen des Widerrufsrechts
- Informationen über die Verwendung der Daten für Entscheidungen, die ausschließlich auf automatisierter Verarbeitung basieren, einschließlich Profiling gemäß Art. 22 Abs. 2 DS-GVO
- mögliche Risiken von Datenübertragungen in Drittstaaten ohne Angemessenheitsentscheidung oder angemessene Garantien, Art. 49 Abs. 1 lit. a DS-GVO

Rechtmäßigkeit der Verarbeitung

Praxisfrage: Müssen bereits erteilte Einwilligungen im Rahmen der Geltung der DSGVO erneuert werden?

- nein, Alt-Einwilligungen gelten grundsätzlich weiter
- aber prüfen, ob diese Einwilligungen den Vorgaben der DSGVO entsprechen oder ob von Einwilligung jahrelang kein Gebrauch gemacht wurde
- empfehlenswert Einholung neuer Einwilligungen, wenn es passt

Rechtmäßigkeit der Verarbeitung

Besondere Kategorien
Art. 9 in Kurzform

Die Verarbeitung besonderer Kategorien personenbezogener Daten ist verboten, es sei denn (z.B.)

- Betroffener hat wirksam eingewilligt oder
- es gibt ein arbeitsrechtliches Erfordernis oder
- Betroffener hat Daten öffentlich gemacht

Besonders schutzbedürftig sind alle Angaben, die direkt oder indirekt Informationen zu den in Art. 9 DS-GVO angegebenen Datenkategorien vermitteln (z. B. Einnahme von Medikamenten, körperliche oder geistige Verfassung, regelmäßiger Besuch einer bestimmten Kirche)

Verarbeitungsverzeichnis

Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DSGVO

Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern müssen kein Verzeichnis von Verarbeitungstätigkeiten führen, es sei denn

- der Verantwortliche bzw. Auftragsverarbeiter führt Verarbeitungen personenbezogener Daten durch, die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (dazu gehören regelmäßig Fälle von Scoring und Überwachungsmaßnahmen) oder
- die nicht nur gelegentlich erfolgen (z.B. die regelmäßige Verarbeitung von Mandanten- oder Beschäftigtendaten) oder
- die besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, usw.) oder strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO betreffen

Fazit: Das Führen eines Verarbeitungsverzeichnisses sollte in jeder Anwaltskanzlei erfolgen!

Verarbeitungsverzeichnis

Inhalt des Verzeichnisses

Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters sowie eines etwaigen Datenschutzbeauftragten;

- die Zwecke der Datenverarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch offen gelegt werden, einschließlich möglicher Empfänger in Drittländern oder bei internationalen Organisationen;
- falls geschehen, die Dokumentation der Übermittlung von personenbezogenen Daten an ein Drittland oder an internationale Organisationen, einschließlich der Angaben des betreffenden Drittlandes oder der betreffenden internationalen Organisationen;
- falls möglich, die Fristen für die Löschung der verschiedenen Datenkategorien;
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherheit (Verschlüsselungsverfahren) gemäß Art 32 DSGVO.

ausgefülltes Muster-Verarbeitungsverzeichnis für die Anwaltskanzlei:
https://anwaltverein.de/de/praxis/datenschutz

Analyse des Verarbeitungsverzeichnisses

- Datensparsamkeit: Ist die Vorhaltung von Daten und deren Verarbeitung tatsächlich notwendig?
- Datenrichtigkeit: Ist gewährleistet, dass beispielsweise Adressdaten stets auf dem neuesten Stand sind, Fehler berichtigt und unrichtige Daten gelöscht werden?
- Rechtmäßigkeit: Lässt sich die Datenverarbeitung auf einen der Gründe des Art. 6 Abs. 1 DSGVO stützen? Dient die Datenverarbeitung der Vertragserfüllung? Gibt es Einwilligungen der Betroffenen? Lässt sich die Datenverarbeitung durch eigene „berechtigte Interessen“ oder durch „berechtigte Interessen“ der Mandanten legitimieren?
- Löschfristen: Werden Daten gelöscht, sobald sie nicht mehr benötigt werden? Gibt es eine Löschroutine, die eine rechtzeitige Löschung jeweils gewährleistet?
- Zugriffsrechte: Haben ausschließlich Mitarbeiter Zugriff zu den Daten, die die Daten für ihre jeweiligen Aufgaben benötigen?
- Zugangskontrolle: Sind die Rechner in der Kanzlei ausreichend gegen den Zugang durch Unbefugte geschützt?

Auftragsverarbeitung

Art.28 Abs.1 DSGVO

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Art. 28 Abs.3 DSGVO: sieht Vertrag zwischen Verantwortlichem und Auftragsverarbeiter vor

Auftragsverarbeiter

Praxisfrage: Wie ermittle ich, ob jemand für das Unternehmen Auftragsverarbeiter ist und was mache ich dann?

1. aus der Buchhaltung Abrechnungsliste vorlegen lassen und auf dieser Grundlage prüfen, wer pbD verarbeitet und als AV in Betracht kommt

Beispiele für Auftragsverarbeitung:

- DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren
- Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des CloudBetreibers erforderlich ist
- Prüfung oder Wartung (z. B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

keine Auftragsverarbeitung: z. B. Einbeziehung eines Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer); für Übermittlung muss Rechtsgrundlage gegeben sein (z.B. Art. 6 DSGVO); Verarbeiter sind selbst Verantwortliche

auch keine AV: z. B. Reinigungsdienst, wenn Personal nur bei Gelegenheit auf Bildschirm blicken kann

Auftragsverarbeiter

2. Abschluss eines Auftragsverarbeitungsvertrages mit dem AV

- Erfüllung der Anforderungen aus Art. 28 Abs.3 DSGVO

vor allem:

Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kreis betroffener Personen, Umfang der Weisungsbefugnisse, Pflichten und Rechte des Verantwortlichen, Pflichten des Auftragsverarbeiters:

Wichtiger Bestandteil des Vertrages ist eine Anlage zu den technischen und organisatorischen Maßnahmen, mit denen der Auftragnehmer Datenschutz und Datensicherheit der ihm überlassenen Daten gewährleistet

Transparenz- und Informationspflichten

Art.13 DSGVO - Informationspflichten

- sofort bei Erhebung der Daten beim Betroffenen

- Folgende Angaben müssen u.a. enthalten sein:

- Name und Kontaktdaten des Verantwortlichen (ggf. auch des Vertreters) und Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- Zweck und Rechtgrundlage der Verarbeitung und Dauer der Speicherung
- Berechtigte Interessen (bei Verarbeitung nach Art. 6 DSGVO)
- Übermittlung in Drittland oder an internationale Organisation
- Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und auf Datenübertragbarkeit
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- Information, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und mögliche Folgen der Nichtbereitstellung

Tranparenz- und Informationspflichten

Praxisfrage: Wie kann ich die Informationspflichten rechtzeitig erfüllen?

- Information in Mandatsbedingungen
- auch im Rahmen von Eingangsbestätigungen denkbar
- Information auf der Website in den Datenschutzbestimmungen
- Telefon: Verweis auf leicht zu merkende Internetadresse

Inhalt:

https://anwaltsblatt.anwaltverein.de/files/anwaltsblatt.de/Dokumente/2018/s0192_1_t8938.html

Transparenz- und Informationspflichten

Art. 14 DSGVO - Informationspflicht bei Erhebung pbD über Dritte

- ähnlich wie Art.13, aber Mitteilung an Betroffenen erforderlich, wo die Daten erhoben wurden
- Mitteilungsfristen;

1. unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,
2. falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,
3. falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

aber: Art. 14 Abs.5 DSGVO, § 29 BDSG Sondervorschrift für Berufsgeheimnisträger: idR keine Mitteilungspflicht

Betroffenenrechte

Auskunftsrecht, Art. 15 DSGVO

Folgende Informationen fallen unter das Auskunftsrecht

- Zwecke der Datenverarbeitung
- Kategorien der Daten und Dauer der Speicherung
- Empfänger oder Kategorien von Empfängern
- Recht auf Berichtigung, Löschung und Widerspruch
- Beschwerderecht bei einer Aufsichtsbehörde
- Herkunft der Daten (wenn nicht bei Betroffenen erhoben)
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling
- Übermittlung in Drittland oder an internationale Organisation

Form der Auskunft: Kopie aller personenbezogenen Daten auf gängigem elektronischem Weg (bei Antrag in elektronischer Form), auch andere Formen möglich. Aber: Identitätsprüfung!

Frist: unverzüglich, spätestens binnen eines Monats

Betroffenenrechte

Recht auf Berichtigung, Art. 16 DSGVO

Gibt den Betroffenen die Möglichkeit, die Korrektur oder Vervollständigung seiner personenbezogenen Daten ohne unangemessene Verzögerung zu verlangen

Recht auf “Vergessen werden”, Art.17 DSGVO

pbD müssen gelöscht werden, wenn

- sie für den Zweck der Verarbeitung nicht mehr erforderlich sind oder
- eine Einwilligung widerrufen wurde oder
- eine unrechtmäßige Verarbeitung vorliegt

Allerdings können gesetzliche Aufbewahrungspflichten oder berechtigte Interessen des Verantwortlichen (Rechtsverfolgung) entgegenstehen.

Betroffenenrechte

Recht auf Datenübertragbarkeit, Art. 20 DSGVO

- Betroffener hat das Recht, von ihm zur Verfügung gestellte Daten von einer automatisierten Anwendung auf eine andere Anwendung zu übertragen
- Ziel ist es, dass Betroffene dadurch leichter von einem Anbieter zu einem anderen wechseln können
- ohne dass es zu Verlust ihrer Daten kommt

Bei Anwälten: ehemaliger Mandant verlangt Übertragung der über ihn gespeicherten Daten zu seinem neuen Anwalt

Betroffenenrechte

Widerspruch, Art. 21 EU-DSGVO

- Betroffene kann jederzeit gegen die Verarbeitung von ihn betreffender personenbezogener Daten und Profilings Widerspruch einlegen
- speziell, wenn diese für Werbung benutzt werden (Abs.2)

Dies bedeutet, das der Verantwortliche die personenbezogenen Daten dann nicht mehr verarbeiten darf

Ausnahmen bestehen nur beim Nachweis zwingender schutzwürdiger Gründe für die Verarbeitung, z.B. wenn diese der Geltendmachung von Rechtsansprüchen dient

- Hinweispflicht auf Widerspruchsmöglichkeit

Datensicherheit

Verschlüsselung der E-Mail-Kommunikation mit Mandant zwingend erforderlich gemäß Art.32 DS-GVO?

Hamburger Datenschutzbehörde: **JA!**

- Die Versendung von unverschlüsselten E-Mails, die personenbezogene Daten enthalten, insbesondere für Angehörige von Berufsgruppen, die auch einer strafrechtlich sanktionierten Schweigepflicht nach § 203 StGB unterliegen, ist nach nicht nur bedenklich, sondern stellt ein ungeeignetes Kommunikationsmittel dar
- Mandant kann in unverschlüsselte Kommunikation nicht einwilligen
- Unter der DSGVO ist eine solche Kommunikation strafbewehrt

https://www.datenschutzbeauftragter-info.de/wp-content/uploads/2018/02/schreiben-der-aufsichtsbehoerde.pdf

Hans. RAK Hamburg: **NEIN!**

Berufsrechtlich schließt die Einwilligung des Mandanten in die unverschlüsselte Kommunikation und den Austausch seiner personenbezogenen Daten einen Verstoß gegen die Verschwiegenheitsverpflichtung (§ 2 Abs.3 lit.a BORA) aus. Nichts anderes gilt im Datenschutzrecht Nach Art. 32 DS-GVO ist Verhältnismäßigkeitsprüfung durchzuführen.

http://www.rak-hamburg.de/mitglieder/mitgliederservice/meldungen/id/36

Datensicherheit

Mindestanforderung E-Mail: Mandanten aufklären und Möglichkeit der verschlüsselten Übermittlung anbieten

Beispiel:
Die Sicherheit von Übermittlungen via E-Mail kann nicht garantiert werden. Via E-Mail übermittelte Informationen können abgefangen oder geändert werden, verloren gehen oder zerstört werden, verspätet oder unvollständig ankommen, oder Viren enthalten. Der Absender übernimmt daher keine Gewähr für Irrtümer oder Auslassungen jeder Art im Inhalt sowie sonstige Risiken, die auf die Übermittlung via E-Mail zurückzuführen sind.
Wir bieten auf Wunsch jedoch die Möglichkeit einer verschlüsselten Kommunikation nach dem Stand der Technik. Derzeit bestehen bei uns hierfür folgende Möglichkeiten der verschlüsselten Kommunikation per E-Mail […(z.B. PGP)…] bzw. via verschlüsseltem Upload auf einen von uns administrierten sicheren Server über [… (z.B. e-Akte/Webakte, WebAttach, ownCloud etc.)…]. Wenn Sie Verschlüsselung nutzen möchten, vereinbaren Sie bitte vorab mit uns die einzusetzende Technik und das Procedere. Senden Sie uns weiterhin unverschlüsselte Mails und Attachments zu, stellt dies einen eigenverantwortlichen Verzicht auf die Möglichkeit einer technischen Sicherstellung von Integrität, Authentizität und Vertraulichkeit dar.

Die Aufsichtsbehörden

- Formelle Anforderungen in Art. 51ff. DSGVO geregelt
- Mit Anwendung der DS-GVO kommt eine Vielzahl neuer Aufgaben und Herausforderungen auf die Aufsichtsbehörden zu. Den Aufsichtsbehörden werden hierfür gemäß Art. 52 Abs. 4 DS-GVO die notwendigen “personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen” zur Verfügung gestellt
- das heisst im Ergebnis: mehr Prüfungen in Unternehmen

Die Aufsichtsbehörden

Art. 57 Abs.1 DSGVO

- Überwachung und Durchsetzung
- Öffentlichkeitsarbeit/ Aufklärung
- Aufklärung von Unternehmen zu datenschutzrechtlichen Pflichten
- Klassifizierung von Datenverarbeitungsprozessen mit oder ohne zwingender Datenschutz-Folgenabschätzung
- Genehmigung von Standardvertragsklauseln für Datentransfers ins EU-Ausland

Die Aufsichtsbehörden

Art. 58 DSGVO, Befugnisse

- verfügen über Untersuchungsbefugnisse
- Umfassender Informationsanspruch
- Datenschutzüberprüfungen
- Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und –geräte
- verfügen über Abhilfebefugnisse, bei beabsichtigten Verarbeitungsvorgängen, die voraussichtlich gegen DSGVO verstoßen
- Verwarnung bei Verstößen
- Anweisung, den Anträgen von Betroffenen bei berechtigtem Anspruch zu entsprechen
- Verarbeitungsverbot/ Löschanweisung

Die Aufsichtsbehörden

Sanktionen

Art. 83 DS-GVO: erhebliche Verschärfung

- bei Verstößen gegen organisatorische Regelungen bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes
- bei Verstößen gegen die Grundsätze der DS-GVO, Rechtmäßigkeit der Datenverarbeitung, Rechte des Betroffenen, Missachtung Anweisung DS-Behörde bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes

Art. 82 DS-GVO: auch immaterielle Schäden sind zu ersetzen

Die Aufsichtsbehörden

Bußgelder sollen abschrecken

Bemessung der Höhe unter Berücksichtigung von

- Art, Schwere und Dauer des Verstoßes sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens
- Vorsätzlich oder fahrlässig
- Erfolgter Schadensminderung
- TOM – technisch-organisatorische Maßnahmen
- Frühere Verstöße
- Zusammenarbeit mit Behörden

Beschäftigtendatenschutz

Neue Regelungen BDSG

- Art. 88 DSGVO erlaubt Mitgliedstaaten durch Rechtsvorschriften oder Kollektivvereinbarungen spezifischere Vorschriften zum Beschäftigtendatenschutz
- aber nach Art. 88 Abs.2 DSGVO müssen gewisse Mindeststandards zum Schutz personenbezogener Daten eingehalten werden (angemessenes Schutzniveau)
- Bundesdatenschutzgesetz wird reformiert durch Datenschutz-Anpassungsgesetz
- Inkrafttreten gleichzeitig mit DSGV am 25.05.2018
- Für Beschäftigungsverhältnisse nun bedeutsam: § 26 BDSG (im Grunde der “alte” § 32 BDSG mit Ergänzungen)

Neue Regelungen BDSG

§ 26 Abs.1 S.1 BDSG
(fett= neu)

Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung **oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten** erforderlich ist.

- lückenhafte bisherige Regelung wurde ergänzt: mit dieser Regelung dürfen auch Betriebsräte Beschäftigtendaten verarbeiten
- war bislang auch möglich, aber ohne klare gesetzliche Regelung

Neue Regelungen BDSG

§ 26 Abs.1 S.2 BDSG

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Neue Regelungen BDSG

§ 26 Abs.2 BDSG (neu)

Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer **Einwilligung**, so sind für die **Beurteilung der Freiwilligkeit** der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende **Abhängigkeit** der beschäftigten Person sowie die **Umstände**, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. **Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.** Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären

Neue Regelungen BDSG

rechtlicher/wirtschaftlicher Vorteil

- in Fällen freiwilliger Leistungen des Arbeitgebers denkbar
- betriebliche Sozialleistungen sein oder das Angebot von Leistungen im Rahmen von Betriebssport oder Gesundheitsvorsorge.

Verfolgung gleichgerichteter Interessen

- Aufnahme von Fotografien oder Videos auf Firmenveranstaltungen oder sonstigen Ereignissen für die Beschäftigten
- Anlegen von Profilen in firmeninternen sozialen Netzwerken

Neue Regelungen BDSG

bei Datenverarbeitung von Beschäftigten in der Kanzlei beachten:

- Beschäftigte neben der Verpflichtung zur Verschwiegenheit auch auf Datengeheimnis verpflichten
- für Veröffentlichung von Daten im Netz (z.B. Fotos auf Website) Einwilligung einholen

Neue Regelungen BDSG

§ 26 Abs.3 BDSG: Verarbeitung besonderer Kategorien von Daten zulässig,

- wenn zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht/soziale Sicherheit/Sozialschutz erforderlich und
- kein Grund zur Annahme besteht, dass schutzwürdiges Interesse der betroffenen Person an Ausschluss der Verarbeitung überwiegt

besondere Kategorien von Daten

- Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen
- Daten, die die genetischer/biometrischer Art sind und die Identifizierung eines Beschäftigten ermöglichen
- Daten, die die Gesundheit des Beschäftigten betreffen
- Daten, die Aussagen zum Sexualleben/sexueller Orientierung enthalten

Neue Regelungen BDSG

§ 26 Abs.4 BDSG: Verarbeitung personenbezogener Daten aufgrund von Kollektivvereinbarungen zulässig, aber Art. 88 Abs.2 DS-GVO zu beachten

§ 26 Abs.5 BDSG: geeignete Maßnahmen zur Wahrung der Grundrechte

§ 26 Abs.6 BDSG: Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt

§ 26 Abs.7 BDSG: Grundsätze gelten auch für personenbezogene Daten außerhalb Dateisystemen

§ 26 Abs.8 BDSG: Definition Beschäftigte

Betroffenenrechte

Erfüllung Informationspflichten Art.13, 14 DSGVO im Beschäftigungsverhältnis

- Anlage zum Arbeitsvertrag
- Betriebsvereinbarung
- Intranet

Bewerbermanagement

- bei Online-Bewerberportal dort Hinweis (ähnlich AGB)
- Information auch im Rahmen der Eingangsbestätigung denkbar

Videoüberwachung

- Sondervorschrift § 4 Abs.2 BDSG, daher nur eingeschränkte Infopflicht

Betriebsvereinbarungen

Änderungsbedarf

- Transparenz: Beschäftigte müssen durch Betriebsvereinbarungen in für sie leicht zugänglicher Weise, sowie in einfacher und verständlicher Sprache über die sie betreffenden Datenverarbeitungen aufgeklärt werden
- Einsatz von Überwachungstechnik: Betriebsvereinbarung soll Regelungen enthalten, die diese Form der Überwachung so weit wie möglich ausschließt.Daher sollten die technischen System verbindlich so konfiguriert werden, dass eine Identifikation der Beschäftigten, soweit es der Zweck zulässt, ausgeschlossen wird (z.B. tw.Schwärzung von Kamerabildern. Daneben spielen Löschfristen udn Zugriffsberechtigungen eine Rolle.
- Einhaltung der Vorschriften der DS-GVO: Aufführung der entsprechenden Regelungen der Arr.12-23 DS-GVO
- Kosmetik: Bereinigung von alten Gesetzesregelungen
- Prüfungen von im Zusammenhang mit BV erteilten Einwilligungen

Fazit Anwaltskanzlei

- Datenschutzbeauftragter ja/nein
- Website Datenschutzbestimmungen
- Informationspflichten Mandant
- Verarbeitungsverzeichnis erstellen und korrekte Verarbeitung prüfen
- Auftragsverarbeitungsverträge abschließen
- E-Mail: Verschlüsselungsfrage lösen

Unterstützung von Mandanten bei Umsetzung von Anforderungen von DSGVO und BDSG 2018

- Anwälte als externe Datenschutzbeauftragte?
- Überarbeitung Website/Datenschutzbestimmungen
- Entwurf Datenschutzrichtlinien Unternehmen
- Prüfung von Einwilligungserklärungen
- Entwurf/Änderung von Auftragsverarbeitungsverträgen
- Anpassung Arbeitsverträge
- Anpassung/Erstellung von Betriebsvereinbarungen

Vielen Dank für Ihre Aufmerksamkeit!

Rechtsanwalt Christian Oberwetter
esb Rechtsanwälte
hamburg@kanzlei.de
www.kanzlei.de