Herzlich willkommen zum
AOK Seminar

Datenschutz

- DSGVO: 1 Jahr nach dem Going live -

Anwaltskanzlei für Wirtschaftsrecht

Der Referent, **Rechtsanwalt Dr. Steffen Häussler,** ist Partner der Kanzlei MACKH | LANG Rechtsanwälte, die schwerpunktmäßig kleine und mittlere Unternehmen betreut. RA Dr. Häussler ist im Bereich des Wirtschaftsrechts neben dem Handelsrecht vor allem im IT-Recht, Arbeitsrecht / Compliance tätig.

Dr. jur. Steffen Häussler, LL.M.
Rechtsanwalt
Fachanwalt für IT-Recht
Fachanwalt für Versicherungsrecht

MACKH | LANG Rechtsanwälte
Partnerschaft mbB | AG Stuttgart PR 720457
Mercedesstraße 35 | 71384 Weinstadt-Endersbach
Telefon: 07151/95942-0 | Telefax: 07151/95942-20
mail@mackh-lang.de | www.mackh-lang.de

Anwaltskanzlei für Wirtschaftsrecht

- Die Kanzlei betreut u.a. **kleine und mittlere Unternehmen auf allen wichtigen Rechtsgebieten**. Betreut werden freilich nicht nur die Unternehmen selbst, sondern auch deren **Inhaber, Geschäftsführer, sonstige Führungskräfte usw.** !
- Neben dem eigentlichen **Wirtschaftsrecht** werden **alle sonstigen wichtigen Bereiche** wie Familien- und Erbrecht, Verkehrsrecht usw. abgedeckt. Auch Unternehmer, Führungskräfte und Mitarbeiter für die der Führerschein besonders wichtig ist, fahren manchmal zu schnell. Auch sind für diese Personengruppe Eheverträge, „Unternehmertestamente“ usw. besonders wichtig.
- Insbesondere bei Umstrukturierungen, Unternehmenskäufen und Nachfolge-regelungen werden MACKH | LANG Rechtsanwälte auch als „Berater Ihrer Berater“ tätig bei der Abdeckung der **Schnittstellen zwischen Steuerrecht und dem Gesellschafts- und Handelsrecht, Arbeits- und Sozialversicherungsrecht, Erb- und Familienrecht etc.** Zur Abrundung wird ein spezielles **Firmeninkasso** angeboten.

Allgemeines

Datenschutz ist eine Abwägung der Interessen des Betroffenen (allgemeines Persönlichkeitsrecht) gegen die Interesse des Daten Verarbeiters.

Personenbezogene Daten: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen zu einer Kennnummer, zu Standortdaten, zu einer Online Kennung identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind

Abgrenzung: **Anonymisierung** und **Pseudonymisierung**

In der Praxis liegt zumeist (nur) eine Pseudonymisierung vor, da eine Anonymisierung keinerlei Rückschlüsse auf Personen mehr zulässt, auch nicht mittelbar über Codes, Schlüssel, Kennungen etc. Damit ist das Datenschutzrecht anwendbar.

Datenschutz bezieht sich auf viele Bereiche:

- Fragen zum Datenschutzbeauftragten**;**
- Den Umgang mit den Aufsichtsbehörden;
- Die Betroffenenrechte;
- Der Beschäftigtendatenschutz;
- Die technischen und organisatorischen Massnahmen zur Umsetzung (TOMs);
- Die Auftragsdatenverarbeitung;
- Basisdokumente, wie die Verfahrensübersicht oder Einwilligungserklärungen;
- Datenschutzaudits;
- Der Datenschutz im Marketing („Stichwort „double opt in“);
- Die datenschutzkonforme Website;
- Implementierung eines Datenschutzmanagements.

Seit dem 25.05.2018 gilt die neue Datenschutzgrundverordnung = EU-DSGVO

Neuerungen u.a.:

- einheitliche Mindeststandards in der EU, was den Datenschutz anbelangt; Auch US Firmen müssen sich daran halten („safe harbour Problematik“)
- Stärkere Nutzerrechte (leichterer Zugang zu den Daten betreffend die eigene Person: Information / Auskunft / Berichtigung / Löschung;
- Das Mindestalter für die Abgabe einer rechtswirksamen Erklärung zur Einwilligung in die Verarbeitung personenbezogener Daten wird auf 16 bestimmt (man denke jetzt an Jugendliche und facebook, Instagram & Co.; In diesem Zusammenhang z.B.: „Recht auf Vergessenwerden“
- Höhere Bussgelder;
- Benennung eines Datenschutzbeauftragen wird notwendig;
- Verfahrensverzeichnis muss erstellt werden (macht DSB).

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a) DSGVO

Zweckbindung (Art. 5 Abs. 1 lit. b) DSGVO)

Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO)

Richtigkeit (Art. 5 Abs. 1 lit. d) DSGVO)

Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO)

Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO)

Datenverarbeitung nur zulässig wenn es die Verordnung oder ein anderes Gesetz zulässt; „Verbot mit Erlaubnisvorbehalt.“

Die wichtigsten Erlaubnistatbestände nach Art 6 DSGVO:

Einwilligung des Betroffenen ; Art 7, 8 DSGVO. Mindestalter 16 Jahre,

Verarbeitung ist zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich.

Die Verarbeitung ist zur Erfüllung rechtlicher Verpflichtungen notwendig

Zur Wahrung schutzwürdiger, berechtigter Interessen wenn keine schutzwürdigen Interessen des Betroffenen überwiegen

Besondere Kategorien von Daten dürfen nicht verarbeitet werden; s. Art. 9 DSGVO. Aber: Ausnahmen s.o. beachten „Verbot mit Erlaubnisvorbehalt.

Unternehmen haben eine **Informationspflicht**, Art. 13, 14 DSGVO: es müssen u.a. folgende Informationen mitgeteilt werden: Name und Kontaktdaten des DSB, Zwecke der Rechtsgrundlage der Datenverarbeitung, ggf. Darstellung der berechtigten Interessen, Dauer der Datenspeicherung, Datenübermittlung ins Ausland

Betroffene haben ein umfassendes **Auskunftsrecht**, Art 15 DSGVO. Es kann die Aushändigung und Übermittlung der gespeicherten Daten als Kopie und in elektronischer Form verlangt werden.

Der Betroffene hat das Recht auf **Datenportabilität,** Art. 20 DSGVO

Recht auf Löschung, „Recht auf Vergessenwerden“, Art. 17 DSGVO
Voraussetzungen: Die Speicherung der Daten ist nicht mehr notwendig, Der Betroffene widerruft seine Einwilligung zur Datenverarbeitung, oder die Daten unrechtmäßig verarbeitet wurden, eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht,

Das Recht auf Vergessenwerden greift nicht: wenn die freie Meinungsäußerung bzw. die Informationsfreiheit überwiegen, Datenspeicherung der Erfüllung rechtlicher Verpflichtung dient, öfftl. Interesse im Bereich der öffentlichen Gesundheit überwiegt, Speicherung zur Abwehr oder Geltendmachung von Rechtsansprüchen notwendig ist

Der Betroffene hat das Recht auf **Datenportabilität,** Art. 20 DSGVO

Recht auf Löschung, „Recht auf Vergessenwerden“, Art. 17 DSGVO
Voraussetzungen: Die Speicherung der Daten ist nicht mehr notwendig, Der Betroffene widerruft seine Einwilligung zur Datenverarbeitung, oder die Daten unrechtmäßig verarbeitet wurden, eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht besteht,

Das Recht auf Vergessenwerden greift nicht: wenn die freie Meinungsäußerung bzw. die Informationsfreiheit überwiegen, Datenspeicherung der Erfüllung rechtlicher Verpflichtung dient, öfftl. Interesse im Bereich der öffentlichen Gesundheit überwiegt, Speicherung zur Abwehr oder Geltendmachung von Rechtsansprüchen notwendig ist

Vorgaben sind also: **TOMs** (technische und organisatorische Massnahmen, Klärung der **ADV** (Auftragsdatenverarebitung), **Verzeichnis** der Verarbeitungstätigkeiten (Art. 30 DSGVO), **Datenschutzfolgenabschätzung** (Art. 35 DSGVO), **Melde- und Informationspflicht** bei Datenpannen binnen 72 Stunden (Art. 33 DSGVO), **DSB** (Datenschutzbeauftragter) Art 37 DSGVO,

Orientierung für Sie und ihr Unternehmen:

https://www.datenschutzkonferenz-online.de/kurzpapiere.html

1. Verzeichnis von Verarbeitungstätigkeiten:

wesentliche Erwartungen der Behörden zum Inhalt des Verarbeitungsverzeichnisses

„Idealerwartungen“ übersteigen gesetzliche Erfordernisse

2. Aufsichtsbefugnisse / Sanktionen

Untersuchungs- und Abhilfebefugnisse im Verwaltungsverfahren

Kommunikation möglicher Sanktionen und Höhen der Geldbußen gemäß Art. 83 DSGVO

3. Verarbeitung personenbezogener Daten für Werbung

Keine Detailregelung für Werbung

Werbung nach Interessenabwägung

Ohne Einwilligung keine werbliche Nutzung besonderer Datenkategorien

Besondere Grenzen aus § 7 UWG

Fortgeltung von Einwilligungen, Kopplungsverbot bei Einwilligungen für Werbung

4. Datenübermittlung in Drittländer

Feststellung der Angemessenheit des Datenschutzniveaus im Drittland durch die EU-Kommission (Art. 45 DSGVO)

Vorliegen geeigneter Garantien (Art. 46 DSGVO)

Ausnahmen für bestimmte Fälle (Art. 49 DSGVO)

5. Datenschutz-Folgenabschätzung

Was ist eine Datenschutz-Folgenabschätzung nach der DSGVO?

Verarbeitungsvorgang als Ankerzeitpunkt

Erforderlichkeit einer DSFA

Zeitpunkt der Durchführung einer DSFA

Wie kann eine DSFA durchgeführt werden?

6. Auskunftsrecht

Auskunftsrecht als zentrales Recht zur Schaffung von Transparenz

Umfang des Auskunftsrechts

Form, Frist, Kosten der Auskunftserteilung

Grenzen des Auskunftsrechts

Identitätsprüfung

7. Marktortprinzip

Regelungen des Marktortprinzips

Angebot von Waren und Dienstleistungen

Überwachung des Verhaltens einer Person

Weitere Folgen

8. Maßnahmenplan

Bestandsaufnahme

Handlungsbedarf eruieren (Rechtsgrundlagen, Betroffenenrechte, Technikgestaltung, Dienstleistungsbeziehungen, Dokumentationspflichten, DSFA, Meldepflichten, Datensicherheit, Zertifizierungen

Umsetzung

9. Zertifizierung

Sinn und Zweck

Bisherige Erfahrungen der Aufsichtsbehörden

Förderung und Vorteile

Zertifizierungsstellen

Voraussetzungen

Rahmenbedingungen und Ausblick

10. Informationspflichten bei Dritt- und Direkterhebung

Bedeutung der Informationspflichten

Informationspflichten bei Direkterhebung

Informationspflichten bei Dritterhebung

Zweckänderung und Übermittlung

Zeitpunkt der Informationspflichten

Form und Nachweis der Informationspflichten

11. Recht auf Vergessenwerden

Löschungspflicht

Ausnahmen von der Löschungspflicht

Beschränkungen des Löschungsanspruches

12. Datenschutzbeauftragte (DSB) bei Verantwortlichen und Auftragsverarbeitern

Benennung des DSB

Gemeinsamer DSB

Berufliche Qualifikation und Fachwissen

Form der Bestellung

Stellung des DSB, Aufgaben des DSB, verantwortung des DSB

13. Auftragsverarbeitung

Begriff des Auftragsverarbeiters

Fortbestehende Sonderregelung für Verarbeitung personenbezogener Daten im Auftrag

Regelungen des Art. 28 DSGVO

Vertrag mit Auftragsverarbeitern

Subunternehmer-Einsatz

Neue Pflichten des Auftragsverarbeiters, Wartung und Fernzugriff, Folgen bei Verstössen

14. Beschäftigtendatenschutz

Datenverarbeitung zum Zweck des Beschäftigtenverhältnisses (§26 BDSG)

Einwilligung

Zur Aufdeckung von Straftaten

Besondere Kategorien personenbezogener Daten

Verarbeitung ausserhalb von Dateisystemen

Zweckänderung, Rechtfolgen bei Verstoss.

15. Videoüberwachung

Einschlägige Rechtsnormen

Inhaltliche Voraussetzungen

Transparenz und Hinweisbeschilderung

Speicherdauer und Löschungsgebot

Sichere Gestaltungsmöglichkeit

Echtzeitüberwachung

Formelle Anforderungen

16. Gemeinsam für die Verarbeitung Verantwortliche

Begriff der gemeinsamen Verantwortlichkeit

Keine Privilegierung gemeinsam Verantwortlicher

Abgrenzung zu anderen Fallgestaltungen

Gemeinsame Entscheidung über Mittel und Zwecke der Verarbeitung

Besondere Pflichten und Anwendungsfälle

17. Besondere Kategorien personenbezogener Daten

Qualifizierung als besondere Kategorie personenbezogener Daten

Verarbeitungsverbot mit Ausnahmevorbehalt

Weitere Anforderungen an die Datenverarbeitung

Anforderungen an die datenverarbeitenden Personen

18. Risiko für die Rechte und Freiheiten natürlicher Personen

Begriffserklärungen (Rechte und Freiheiten natürlicher Personen nach DSGVO, Risiko nach der DSGVO)

Risiko und Rechtsfolgen

Risikobeurteilung

Eindämmung des Risikos

19. Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DSGVO

Regelungen nach der DSGVO

Wer muss verpflichtet werden ?

Inhalt der Verpflichtung

Form der Verpflichtung

Erneuerung der Verpflichtung

20. Einwilligung nach der DSGVO

Grundsatz der Freiwilligkeit

Fortgeltung erteilter Einwilligungen

Folgen bei unwirksamer Einwilligung

Besondere Kategorien von Daten und Einwilligung von Kindern / Jugendlichen

Weitere interessante Veröffentlichungen:

Entschließung der DSK zur gemeinsamen Verantwortlichkeit bei Facebook Fanpage Betreibern vom 06.06.2018

Beschluss der DSK zu Facebook Fanpages vom 05.09.2018

Stellungnahme der Datenschutzbehörde NRW: Kommunikation per E-Mail bedarf mindestens der Transportverschlüsselung

Stellungnahme der BfDI zur Zulässigkeit von WhatsApp in der Unternehmenskommunikation

Ausgewählte Themenschwerpunkte:

Beschäftigtendatenschutz

Datenschutzbeauftragter

Datenschutz im Marketing

Erheben, Verarbeiten, Nutzen **personenbezogener Daten** eines Beschäftigten.

Schutz der Persönlichkeitsrechte der Arbeitnehmer an Hand der Kriterien der Erforderlichkeit und der Verhältnismäßigkeit (legitimer Zweck, Geeignetheit, Angemessenheit) der Datenverarbeitung.

FC Bayern überwacht Fanshop Mitarbeiter mit Kameras, auch in vermeintlichen Sozialräumen; ArbG Oberhausen vom 25.02.2016, Az. 2 Ca 2024/15. Zulässig ?

Arbeitgeber überwacht den Browserverlauf und die E-Mails von Arbeitnehmern, u.a. LAG Berlin-Brandenburg vom 14.01.2016, 5 Sa 657/15, EGMR 05.09.2017 Az. 61496/08. Zulässig ?

Die elektronische Personalakte und das Bewerbungsverfahren: Aufbewahrungsrechte, Informationspflichten, Berichtung und Löschung

➡ **Der betriebliche Datenschutz war schon vor der DSGVO wichtig, jetzt rückt er ins Zentrum der Aufmerksamkeit !**

Fall: Ein ausgeschiedener Mitarbeiter beschwerte sich darüber, dass sein personalisierter E-Mail-Account, name@unternehmen.de, nicht unmittelbar nach seinem Ausscheiden gelöscht wurde. Es stellte sich heraus, dass es im Unternehmen keine Regelungen zur Nutzung der Informations- und Kommunikationstechnik (IuK) gab. Die Mitarbeiter gingen davon aus, dass die private Nutzung der betrieblichen IuK gestattet war und wurden auch nicht durch stichprobenartige Kontrollen und daraufhin ausgesprochene Sanktionen vom Gegenteil überzeugt. Als Folge hatte sich die Erlaubnis zur Privatnutzung der IuK durch „betriebliche Übung“ etabliert. Damit war das Unternehmen als Dienstanbieter im Sinne des TKG bzw. TMG anzusehen und dem Fernmeldegeheimnis unterworfen. Der Zugriff auf den E-Mail-Accounts des ausgeschiedenen Mitarbeiters war somit unzulässig. Und dies betraf nicht nur dessen private Mails, sondern natürlich auch seine dienstlichen, denn in seinem Account waren sie nicht auseinanderzuhalten. Ein massives Problem für das Unternehmen!

Fall: Die „freiwillige“ Urinprobe. Der minderjährige Beschwerdeführer befand sich in einem Berufsausbildungsverhältnis. Weil sein Arbeitgeber ihn verdächtigte, Cannabis zu konsumieren, erklärte sich der Beschwerdeführer bereit, sich einem Drogentest zu unterziehen. Der Arbeitgeber sah die Einwilligung als wirksame Rechtsgrundlage zur Verarbeitung der besonderen Arten personenbezogener Daten (Gesundheitsdaten nach § 3 Abs. 9 BDSG bzw. Art. 9 Abs. 1 DSGVO) des Beschäftigten an. Der Arbeitgeber musste eines Besseren belehrt werden. Gegen die Wirksamkeit der Einwilligung sprach im vorliegenden Fall neben der **mangelnden Freiwilligkeit** der Einwilligung und der **Minderjährigkeit** des Beschwerdeführers auch die Beschäftigung im Berufsausbildungsverhältnis**.**

Wer braucht seit 25.05.2018 einen Datenschutzbeauftragten?

Grundlage ist Art 37 EU-DSGVO:

- Kerntätigkeit: Verarbeitungsvorgänge, die aufgrund ihrer Art, Umfang, Zweck eine umfangreiche regelmäßige und systematische Überwachung erforderlich machen. Kerntätigkeit ist jede Tätigkeit, die essentiell für die Erreichung der Ziele des Unternehmens sind. Bsp.: Verarbeitung von Gesundheitsdaten in einem Krankenhaus.
- Kerntätigkeit besteht in umfangreicher Verarbeitung besonderer Kategorien von Daten (Auftragsverarbeiter)
- + **Öffnungsklausel** im nationalen Recht.

➡ Neues BDSG 2018 setzt um: „…soweit **mindestens 10 Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.“ Oder geschäftsmäßige Auftragsdatenverarbeitungen unabhängig von der Anzahl der Personen (Adresshändler, Meinungsforscher).

Wer braucht seit 25.05.2018 einen Datenschutzbeauftragten?

D.h. die 10 Personen Grenze (inkl. Teilzeitkräfte und Leiharbeitnehmer) ergibt sich aus dem BDSG neu 2018 und nicht aus der EU-DSGVO unmittelbar.

Eine freiwillige Benennung bleibt freilich möglich und könnte aus Compliance Sicht Sinn machen…

Ein gemeinsamer Datenschutzbeauftragter für Unternehmensgruppen ist möglich; Art 37 Abs. 2 EU-DSGVO knüpft an den Konzernbegriff an.

Anforderungen und Benennung ?

Anforderungen sind

- berufliche Qualifikation,
- Das Fachwissen auf dem Gebiet des Datenschutzes und der Praxis und
- Die Fähigkeit zur Aufgabenerfüllung

Der interne Datenschutzbeauftragte muss geschult werden
Der externe Datenschutzbeauftragter muss geschult sein.

➡ Neu: die Kontaktdaten des DSB sind zu **veröffentlichen** (Internet / Intranet, **Impressum**).

Die Stellung des Datenschutzbeauftragten

Verpflichtung zur frühzeitigen und ordnungsgemäßen Einbindung

Unterstützungspflicht bei Erfüllung der Aufgaben: Ressourcen, Zugang zu personenbezogenen Daten, Erhaltung des Fachwissens.

Neu:

- Verbot von Anweisungen und Vorgaben; keine Abrufbarkeit oder Benachteiligung
- Unmittelbare Berichtslinie an höchste Managementebene.
- DSB kann auch andere Pflichten wahrnehmen, wenn **kein Interessenkonflikt.**

Die Stellung des Datenschutzbeauftragten

Während die EU-DSGVO nur von „keiner Abrufbarkeit“ spricht, implementierte das BDSG 2018 einen besonderen Kündigungsschutz für den internen DSB; § 38 Absatz 2 BDSG-neu. Eine Probezeit ist unzulässig.

Intern / Extern ?
Intern: Kündigungsschutz. Extern: jedenfalls kein gesetzlicher Kündigungsschutz; Kann „ausgewechselt werden“.

Es scheiden aus: Geschäftsführer, Leiter Personal oder IT und auch wohl Gesellschafter wegen **Interessenskollisionen**. Bußgeldbewährt

Die Aufgaben des DSB

Unterrichtung und Beratung der Beschäftigten hinsichtlich der Pflichten der EU-DSGVO. „Nur“ sog. **Hinwirkungspflicht** keine Entscheidungsgewalt im Unternehmen.

Schulung Mitarbeiter

Beratung der GF / Folgenabschätzung

Koordination mit Aufsichtsbehörden

Neu: Überwachung der Umsetzung der DSGVO

Sanktionen

Bisher: **Bussgeld** bis zu EUR 50.000.- im Regelfall, max. EUR 300.000,00 (§ 43 BDSG)

Neu: bis EUR 10 Mio oder 2 % des weltweiten Jahresumsatzes (Art. 83 Absatz 4 DSGVO). Bei letzterem zielt man wohl auf Google, facebook & Co.

Erstes DSGVO Bussgeld wurde von der LfDI BW im Fall „Knuddels“ verhängt: EUR 20.000.-

International: Krankenhaus wegen Verstosses gegen Art. 32 DSGVO: EUR 400.000.- (Portugal)

Google LLC wegen Verstosses gegen Art. 5, 13 und 14 DSGVO: EUR 50 Mio. (Frankreich)

Beschäftigtendatenschutz

In der täglichen Arbeit des DSB liegt ein Schwerpunkt in der Durchführung der Arbeitsverhältnisse mit den Angestellten

§ 32 BDSG regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für die Zwecke des Beschäftigungsverhältnisses. Daneben ist § 28 BDSG anwendbar etwa bei der Internetrecherche bzgl. Bewerbern, Maßnahmen bei Corporate Governance

Dies setzt Erforderlichkeit und Verhältnismäßigkeit voraus, Abwägung zwischen berechtigten Interessen des AG und schutzwürdigen Interessen des AN. Im Zweifel überwiegt das schutzwürdige Interesse des AN.

Beschäftigtendatenschutz

Zur Verarbeitung personenbezogener Daten des AN wird die Einwilligung im Rahmen der Begründung des Arbeitsverhältnisses gegeben. Es empfiehlt sich, hinsichtlich etwaiger Foto- oder Videoveröffentlichungen sich vom Arbeitnehmer gesondert eine Einwilligung geben zu lassen, deren Wirkung im Zweifel sogar über die Beendigung des Arbeitsverhältnisses hinausreicht. Veröffentlichte ältere Firmenfotos müssen so nicht gelöscht werden.

Anerkannt ist es, dass Betriebsvereinbarungen und Tarifvereinbarungen Datenschutzrechtliche Fragen verbindlich geregelt werden können.

Beschäftigtendatenschutz

Der AG erhebt, verarbeitet, nutzt personenbezogene Daten von Bewerbern in der Bewerbungsphase

Kenntnisnahme durch so wenig Personen wie möglich (gezielte Bewerbung) und soviel Personen wie nötig (Initiativbewerbung)

Grund: Erforderlichkeit der Datenverarbeitung / Zweckbindung

Beschäftigtendatenschutz

Das Bewerbungsverfahren ist dann geprägt durch den Komplex des Fragerechts des AG.

Zulässiger Umfang von Fragen richtet sich nach § 32 Absatz 1 Satz 1 BDSG sowie nach dem Allgemeinen Gleichstellungsgesetz (AGG)

Grundsätze des BAG zum Fragerecht des AG. Strenger Massstab bei der Erforderlichkeitsprüfung. Diskriminierungsrelevante Daten nach dem AGG dürfen nur dann erhoben werden, wenn sie von objektiver / sachlicher Bedeutung für die ausschlaggebende Stelle sind

Beschäftigtendatenschutz

Typische Fragen:

- Gesundheit des Bewerbers (+) wenn für Stelle erforderlich
- Religionszugehörigkeit (-) grundsätzlich unzulässig
- Politische Einstellung (-/+) wenn Voraussetzung für die Stelle
- Qualifikation / frühere Tätigkeit (+) sofern Bezug zur konkreten Tätigkeit
- Vermögensverhältnisse (-) grundsätzlich unzulässig
- Vorstrafen (+) falls konkreter Bezug zur konkreter Tätigkeit
- Sprachkenntnisse (+) bei Bezug zur konkreten Tätigkeit
- Schwerbehinderung, Schwangerschaft (-) es sei denn, wenn im Zusammenhang mit der Stelle, wohl aber erst nach der Einstellung

Beschäftigtendatenschutz

Social Media und Datenschutz von Bewerbern / Recherche

Grundsätze: Daten, welche frei zugänglich und vom Bewerber eingestellt sind. Erhebung (+), wenn Bewerber darauf hingewiesen wird (z.B. in der Stellenausschreibung)

Daten frei zugänglich aber nicht vom Bewerber eingestellt: Erhebung grundsätzlich (-), es sei denn Bewerber hat im Vorstellungsgespräch die Möglichkeit zur Richtigstellung

Daten aus beruflichen Netzwerken, welche vom Bewerber eingestellt: Erhebung (+) da Nutzung des Netzwerks beruflichen Zwecken dient

Daten des Bewerbers in privaten sozialen Netzwerken: Erhebung grundsätzlich (-), wegen des privaten Charakters solcher Netzwerke

Beschäftigtendatenschutz

Bewerbungsunterlagen abgelehnter Bewerber sind zurückzugeben (Papierform) oder zu löschen (elektronische Speicherung)

Aufbewahrungsfrist bis zu 6 Monaten nach Beendigung des Bewerbungsverfahrens

AN kann evtl. Schadensersatzanspruch nach der Ablehnung geltend machen. Die Frist für die Geltendmachung beträgt 2 Monate. Aufsichtsbehörden halten Aufbewahrung bis zu 6 Monaten deshalb für zulässig.

Daten sind bis zur Löschung gemäß § 35 Absatz 3 Nr. 1 BDSG gesperrt aufzubewahren.

Beschäftigtendatenschutz

Die Grundprinzipien der Personalakte:

Vertraulichkeitsprinzip: sichere Verwahrung, Schutz vor unbefugtem Zugriff

Prinzip der Richtigkeit und Vollständigkeit: unrichtige Daten, Recht des AN auf Gegendarstellung § 83 Absatz 2 BetrVG)

Gleichbehandlungsgrundsatz: gleicher Umfang der Aktenführung bei allen Mitarbeitern

Zweckbindungsgrundsatz: gesetzliche Nachweispflicht des AG

Transparenzgrundsatz: Einsichtsrecht des AN, § 83 Absatz 1 BetrVG

Beschäftigtendatenschutz

Typische Verarbeitungskonstellationen im Arbeitsverhältnis:

Systeme zur **Arbeitszeiterfassung**: i.d.R. erforderlich und verhältnismäßig für die Leistungskontrolle durch den AG. Vereinbarung von Vertrauensarbeitszeiten ist kein vergleichbares Mittel. Unklar bei Zeiterfassung mit Bildern der AN zur Identitätsfestellung, wohl (-)

Ortung von Mitarbeitern: i.d.R. erforderlich und verhältnismäßig für Diebstahlsschutz bei wertvollen Frachtgegenständen oder Arbeitsmitteln. Hohe Anforderungen an Erforderlichkeit und Verhältnismäßigkeit. Beschäftigte müssen hierüber unterrichtet werden, kein Eingriff in den Kernbereich privater Lebensgestaltung. Bei Ortung auch privat genutzter Gegenstände. Keine Ortung nach Dienstschluss und während der Pausenzeiten

Film- und Fotoaufnahmen des AN: Veröffentlichung nur mit Einwilligung des AN. Bei Widerruf Abwägung zwischen den Interessen AN / AG

Beschäftigtendatenschutz

Weitere Verarbeitungskonstellationen, die einen rechtlichen Rahmen durch Datenschutzerklärungen, Betriebsvereinbarungen oder Arbeitsverträge bedürfen:

- Verarbeitung biometrischer Daten (Arbeitszeiterfassung mit Fotos der Mitarbeiter beim „Abstempeln“)
- Chipping von Mitarbeitern
- Smart Car (vernetzte Fahrzeuge)
- Bring your own Device (BYOD)
- Einsatz mobiler Datenträger
- Cloud Computing
- Betriebliches Eingliederungsmanagement
- Whistleblowing

Beschäftigtendatenschutz

Offene Überwachung öffentlich zugänglicher Räume

Öffentlich zugänglicher Raum: Öffentliche Wege, Straßen und Plätze, Teile des Betriebsgeländes, die ohne anderweitige Eintrittskontrolle zugänglich sind, z.B. Kaufhäuser, Empfangsbereiche

Erkennbarkeit der Videoüberwachung: Hinweisschild

Max. 1 Meter Bürgersteig als Nebeneffekt (AG Berlin)

Erstellung eines Datenschutzkonzepts notwendig. Zweck, Dauer und Auswertung muessen festgelegt werden.

Beschäftigtendatenschutz

Zulässige Überwachungszwecke

Wahrnehmung des Hausrechts als berechtigtes Interesse, v.a. im Außenbereich unter erleichterten Voraussetzungen.

Gebäudeschutz, Aufklärung von durch Dritten begangenen Straftaten, Aufklärung von durch Mitarbeiter begangene Straftaten ohne Tatverdacht i.d.R (-)

Beschäftigtendatenschutz

Bewertung der Technik des Kamera Systems

Abwägung verschiedener Interessen

Prüfung der Datenweitergabe an Dritte

Einschränkung und Kenntlichmachung

Interessenabwägung / Speicherdauer

Sicherstellung Betroffenenrechte

Beschäftigtendatenschutz

Überwachung des E-Mail-Verkehrs und der Internetnutzung

Bei Verbot der privater Nutzung: Kontrolle von Verbindungsdaten durch AG
(+) Kontrolle, ob das Verbot eingehalten wird, muss dem AG möglich sein

Einblick in Inhaltsdaten zur Durchführung geschäftlicher Interessen: Zurkenntnisnahme von Inhaltsdaten durch den AG grdsl. (+); i.d.R. können keine privaten Daten betroffen sein aufgrund Verbots.

Eine anlasslose Dauerüberwachung der AN ist **nicht** zulässig

Beschäftigtendatenschutz

Überwachung der E-Mail und Internet Nutzung bei Erlaubnis oder Duldung der privaten Nutzung

Rechtsgrundlage, Erlaubnis: Zusatz im Arbeitsvertrag, Betriebsvereinbarung oder Dienstanweisung. Duldung erzeugt betriebliche Übung als Erlaubnis des AN. Aber. Das Verhalten des AG muss in Kenntnis der Umstände erfolgen, blosse Unkenntnis reicht nicht

Die dauerhafte Missachtung des Verbots privater Nutzung führt nicht zu einer ersetzender Erlaubnis durch betriebliche Übung. Allerdings muss das Verbot klar und eindeutig sein, damit es wirksam ist.

Beschäftigtendatenschutz

Telefonüberwachung: Kontrolle von Verbindungsdaten durch AG (+), Kontrolle ob das Verbot privater Nutzung eingehalten wird, muss dem AG möglich sein.

Inhaltsdaten: heimliches Mithören oder Aufzeichnen von privaten oder geschäftlichen Telefongesprächen ist generell untersagt (auch bei verbotener Privatnutzung). Offenes Mithören oder Aufzeichnen erfordert die Einwilligung des AN und seines Gesprächspartners

In Call Centern wird während der Einarbeitungszeit (Probezeit) das Mithören zur Einarbeitung als zulässig erachtet („Bedienplatzreports“)

Beschäftigtendatenschutz

Nach Beendigung des Arbeitsverhältnisses sind alle Daten des AN zu löschen.

Ausnahme: gesetzliche Aufbewahrungspflichten, Abwicklung von Pensionsansprüchen (30 Jahre). Schadensersatzansprüche (Sperrung)

Beschäftigtendatenschutz

Artikel 88 Absatz 1 EU-DSGVO sieht vor, dass folgende Kontexte im Beschäftigungsverhältnis zu regeln sind, ob durch Arbeitsvertrag, Betriebsvereinbarung oder spezielle Vereinbarungen ist sekundär:

- Einstellung und Erfüllung des Arbeitsvertrages
- Management, Planung und Organisation der Arbeit
- Gleichheit und Diversität am Arbeitsplatz
- Gesundheit und Sicherheit am Arbeitsplatz
- Schutz des Eigentums der Arbeitgeber und Kunden
- Beendigung des Beschäftigungsverhältnisses

Die Auftragsdatenverarbeitung

Übermittlung von Daten innereuropäisch und außereuropäisch. Auftragsverhältnis zwischen Auftraggeber und Auftragnehmer. Erforderlich ist ein schriftlicher ADV Vertrag. Dort müssen Kontrollrechte und Weisungsgebundenheit normiert werden.

Dann erfolgt eine **Privilegierung** der Übermittlung durch die Fiktion der Einwilligung bzw. genauer die sog. **Fiktion** der **Nicht-Übermittlung**

Man betrachtet den Auftraggeber und den Auftragnehmer als Einheit.

Siehe Mustervertrag ADV in der Anlage. Neue Pflichten aus DSGVO: Verzeichniserstellung, TOMs, DSB, Datentransferbeschränkung in Drittländer; Art. 44 DSGVO.

Beschäftigtendatenschutz bei Arbeitsunfähigkeit und betrieblichem Eingliederungsmanagement

Zur Begründung, Durchführung und Beendigung notwendig

Verhältnismäßigkeitsprüfung

Abwägung: Informationsinteresse AG / allg. Persönlichkeitsrecht des AN

Frage: wer hat Zugriff auf die Daten, wie lange werden diese gespeichert.

Recht des Betriebsrates, auch die Gesundheitsunterlagen der Beschäftigten einzusehen im Rahmen von Fragen zum BEM, ist vorhanden.

Regelungsinstrument: Betriebsvereinbarungen

„BV zum innerbetrieblichen Umgang mit AU-Meldungen, ärztlichen Attesten und sonstigen Kranken- und Gesundheitsdaten…“

Datenschutz im Marketing

Werbung abzugrenzen von reiner Service und Vertragskommunikation.

Anwendung des Wettbewerbsrechts neben dem Datenschutzrecht.

Wettbewerbsrecht schützt im UWG die Lauterkeit des Wettbewerbs, das Datenschutzrecht schützt die informationelle Selbstbestimmung

Ausnahmen vom ausdrücklichen Einwilligungserfordernis: Postwerbung mit Kundendaten, Postwerbung mit Daten Dritter, Wettbewerbsrechtliche Ausnahme des § 7 Absatz 3 UWG.

Datenschutz im Marketing

§ 7 Unzumutbare Belästigungen
(1) Eine geschäftliche Handlung, durch die ein Marktteilnehmer in unzumutbarer Weise belästigt wird, ist unzulässig. Dies gilt insbesondere für Werbung, obwohl erkennbar ist, dass der angesprochene Marktteilnehmer diese Werbung nicht wünscht.
(2) Eine unzumutbare Belästigung ist stets anzunehmen
1.
bei Werbung unter Verwendung eines in den Nummern 2 und 3 nicht aufgeführten, für den Fernabsatz geeigneten Mittels der kommerziellen Kommunikation, durch die ein Verbraucher hartnäckig angesprochen wird, obwohl er dies erkennbar nicht wünscht;
2.
bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung,
3.
bei Werbung unter Verwendung einer automatischen Anrufmaschine, eines Faxgerätes oder elektronischer Post, ohne dass eine vorherige ausdrückliche Einwilligung des Adressaten vorliegt, oder
4.
bei Werbung mit einer Nachricht,
a)
bei der die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, verschleiert oder verheimlicht wird oder
b)
bei der gegen § 6 Absatz 1 des Telemediengesetzes verstoßen wird oder in der der Empfänger aufgefordert wird, eine Website aufzurufen, die gegen diese Vorschrift verstößt, oder
c)
bei der keine gültige Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.
(3) **Abweichend von Absatz 2 Nummer 3 ist eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post nicht anzunehmen, wenn**
1.
ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,
2.
der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
3.
der Kunde der Verwendung nicht widersprochen hat und
4.
der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entste

Änderungen nach der DSGVO:

Kein Listenprivileg mehr

Betroffene können jederzeit und ohne Begründung der Verwendung ihrer Daten für Zwecke des Marketings widersprechen

Es wird stärker auf die Zulässigkeit der Verarbeitung abgestellt und die Möglichkeit zum **Widerspruch**, vgl. Art 21 und Art 6 EU-DSGVO

Betroffenem müssen bei Erhebung bestimmte Informationen zur Verfügung gestellt werden; Art. 13 EU-DSGVO

Datenschutzkonforme Website

Nutzer ist vom Diensteanbieter zu Beginn der Nutzung über Art, Umfang und Zweck der Erhebung und Verarbeitung, über die Verarbeitung in Staaten außerhalb des Anwendungsbereichs der RL 95/46 EG in allgemeinverständlicher Form und jederzeit abrufbar zu unterrichten: **Datenschutzerklärung**

Die EU-DSGVO verlangt weiterhin mit den bekannten Materien (Cookies, Social-Plugins, Analyse Tools) datenschutzkonforme Erklärungen

Die DSGVO schreibt den Betreibern nunmehr den Datenschutz vor, durch Technikgestaltung „privacy by design“ und datenschutzfreundliche Einstellungen „privacy by default“

Privacy by design: Datenschutz muss bereits während der Programmierung berücksichtigt werden.

Privacy by default: Datenschutz muss Grundsatz der Datenminimierung enthalten.

Websites für Kinder: Aufklärung in kindgerechter Sprache, für die rechtmäßige Nutzung der Website durch Kinder unter 16 Jahren ist die Einwilligung des Trägers der elterlichen Verantwortung notwendig.

Im Impressum muss der DSB benannt werden. Ebenso die Datenschutzbehörde in der Datenschutzerklärung

Abmahnung, was tun ?

Die richtige Reaktion auf die Abmahnung und die Konsequenzen.

Unterschied zwischen Vertragsstrafe (vertragliche Abrede / Unterlassungserklärung) und Ordnungsgeld (richterlicher Akt / einstweilige Verfügung oder Urteil).

Einstweilige Verfügung und Hauptsacheverfahren

Prävention vor Reaktion

Abmahnung, was tun ?

1. Im Falle eines Verstoßes gegen die Unterlassungsverpflichtung gemäß …… verpflichtet sich der Unterlassungsschuldner eine Vertragsstrafe über EUR 10.000.- pro Verstoß an den Unterlassungsgläubiger zu bezahlen.

2. Im Falle eines Verstoßes gegen die Unterlassungsverpflichtung gemäß ……. Verpflichtet sich der Unterlassungsschuldner eine angemessene Vertragsstrafe an den Unterlassungsgläubiger zu bezahlen die im Verstossfall vom Unterlassungsgläubiger bestimmt und auf Antrag des Unterlassungsschuldners vom zuständigen Gericht auf die Angemessenheit hin überprüft wird.

Haben Sie noch Fragen?

Dann fragen Sie nicht Ihren Arzt oder Apotheker, sondern uns:

MACKH | LANG Rechtsanwälte
Partnerschaft mbB | AG Stuttgart PR 720457
Mercedesstraße 35 | 71384 Weinstadt-Endersbach
Telefon: 07151/95942-0 | Telefax: 07151/95942-20
mail@mackh-lang.de | www.mackh-lang.de




AOK Seminar
– Datenschutzgrundverordnung ein Jahr nach dem Going live

Vielen Dank für Ihr Interesse!
Kommen Sie gut nach Hause!