Blickhan

Datentechnik.de

Beratung zur wirtschaftlichen Einhaltung von
EU-Richtlinien und Gesetzen

Günter W. Blickhan
Dipl.-Ing. REFA-Ing. Betriebsinformatiker
Telefon: 060 733 733
Datenschutz@Blickhan.de

Datenschutz-Dialog
Basis-INFO-SERVICE

→ Wirtschaftliche Einhaltung der EU-DSGVO ←

Blickhan
Datentechnik.de

Beratung zur wirtschaftlichen Einhaltung von EU-Richtlinien und Gesetzen

Mein Support – Ihr Nutzen:

→ Datenschutz@Blickhan.de

- ✓ Individuelle Beratung zur wirtschaftlichen Einhaltung der EU-DSGVO
- ✓ Externer Datenschutzbeauftragter

- ✓ Aktuelle Informationen und Fragen zum Datenschutz

- ✓ Datenschutz-Dialog in der Metropolregion Frankfurt Rhein-Main-Neckar
- ✓ Beratung für verfahrensrechtliche und verfahrenstechnische Maßnahmen in kleinen praxisorientierten Gruppen

Agenda

Geschichte des Datenschutzes

Handlungsbedarf zur EU-DSGVO (DatenSchutzGrundVerOrdnung)

Grundlagen für die Rechtmäßigkeit der Datenverarbeitung

- Anforderungen an Einwilligungen
- Zweckbindung
- Betroffenenrechte
- Dokumentationspflichten
- Sicherheit der Verarbeitung
- Data protection by design und by default
- Datenschutz-Folgenabschätzung
- Konsultation der Aufsichtsbehörde
- Meldepflicht bei Datenpannen
- Unternehmensgruppen
- Auftragsverarbeitung
- Haftung bei der Auftragsverarbeitung
- Zertifizierungen und genehmigte Verhaltensregeln
- Aufsichtsbehörden
- Datenschutzbeauftragter
- Öffnungsklauseln

Was passiert nach dem 25. Mai 2018, wenn nichts passiert?

- Verschärfte Sanktionen

Empfohlene Maßnahmen

EU-DSGVO:
Den kompletten Verordnungstext hat die EU im PDF-Format zum Download veröffentlicht.
→ http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE
→ Quelle: © Europäische Union, http://eur-lex.europa.eu/ , 1998–2017

Geschichte des Datenschutzes

800 v. Chr. bis 1970

Der Bedarf nach Datenschutz bestand bereits 800 v. Chr. und liegt in der ärztlichen Schweigepflicht begründet. Andere Bestimmungen zum Schutz der Privatsphäre kamen erst später auf, wie 200 n. Chr. das Beichtgeheimnis

Weitreichender befasst wurde sich mit dem Datenschutz in den USA in den 1960er Jahren als die Entwicklung der Computertechnologie voranschritt. Das erste Datenschutzgesetz wurde dann am 30. September 1970 in Hessen verabschiedet, welches damit das erste Bundesland mit einem Landesdatenschutzgesetz war

Dieses Datenschutzgesetz beinhaltete den Schutz von elektronisch vorliegenden Daten vor unberechtigter Einsicht Dritter. Mitarbeiter, die Zugriff auf solche Daten haben, obliegen laut Gesetz der Schweigepflicht. Des Weiteren haben die von den Daten betroffenen Personen das Recht, ihre Daten bei Bedarf korrigieren zu lassen. Unter anderem wurde im Datenschutzgesetz festgelegt, dass ein Datenschutzbeauftragter für öffentliche Stellen eingestellt werden muss.

Quelle: http://www.informatik.uni-oldenburg.de/~iug11/rf/geschichte.html

Geschichte des Datenschutzes

1970 bis 1990

1977 wurde das erste Bundesdatenschutzgesetz veröffentlicht

Das BDSG vom 28. Januar 1977 konzentrierte sich ebenfalls auf den Schutz der „personenbezogenen Daten" und war vom Grundgedanken bestimmt, dass staatliche Stellen, aber auch Unternehmen nicht ohne weiteres in das Recht des Einzelnen, allein gelassen zu werden, eingreifen dürfen. Für die Datenverarbeitung öffentlicher Stellen wurde der „Erforderlichkeitsgrundsatz" eingeführt, d.h. es durften nur solche personenbezogene Daten verarbeitet werden, die für die Erledigung der gesetzlichen Aufgabe der Behörde erforderlich waren. Personenbezogene Daten durften zudem nur verarbeitet werden, wenn entweder ein Gesetz dies vorsah oder der Betroffene der Verarbeitung freiwillig zustimmte.

Bis 1981

folgten in Deutschland alle alten Bundesländer und verabschiedeten ebenfalls Landesdatenschutzgesetze.

Quelle: http://www.informatik.uni-oldenburg.de/~iug11/rf/geschichte.html

Geschichte des Datenschutzes

1990 bis 2009

Das aus dem Grundgesetz abgeleitete Grundrecht auf informationelle Selbstbestimmung begründete die Neufassung des Bundesdatenschutzgesetzes im Jahre 1990.

Die Datenschutzgesetze der Länder und des Bundes wurden erneuert, da der Staat Maßnahmen ergreifen musste, um den Bürgern das genannte Recht zu gewährleisten. Nicht nur in Deutschland, sondern auch in der Europäischen Union beschäftigte man sich mit dem Datenschutz.

So beschloss die
EU am 24. Oktober 1995 Rahmenrichtlinien für die nationale Datenschutzgesetzgebung.
Darin wird nicht mehr zwischen gewerblichen und privaten Daten unterschieden, sondern der
Schutz von allgemein wichtigen oder wertvollen Daten steht im Vordergrund.

Für Datenschutzbeauftragte wird in den Richtlinien bestimmt, dass bei neuen Gesetzesentwürfen, die den Datenschutz betreffen, z.B.
Risikoanalysen und Vorabkontrollen durchgeführt werden müssen. Darüber hinaus wird ein angeglichenes Datenschutzniveau bei den EU-Mitgliedsstaaten vorgeschrieben, was die Übertragung personenbezogener Daten innerhalb der Europäischen Union vereinfacht.

In den darauffolgenden Jahren wurde das Internet intensiver als zuvor genutzt, woraus sich die sozialen Netzwerke entwickelten.
Im Juli 2003 entstand MySpace und begründete damit die sozialen Netzwerke, wie man sie heute kennt.
Danach folgten im Februar 2004 Facebook aus den USA und Ende 2005 wurde das Studentenverzeichnis StudiVZ in Deutschland gegründet.

Nach 1990 wurde das Bundesdatenschutzgesetz nicht mehr verändert.

Da die Nutzung des Internets aber seit der ersten Veröffentlichung des Bundesdatenschutzgesetzes stark gestiegen ist, folgte
ab 2009 eine ereignisreiche Zeit für den Datenschutz.

Quelle: http://www.informatik.uni-oldenburg.de/~iug11/rf/geschichte.html

Geschichte des Datenschutzes

1990 bis 2009

Ein weiteres Gesetz neben dem Datenschutzgesetz,
das sich mit der Sicherheit im Internet befasst, ist das
Telemediengesetz (TMG).

Dieses regelt die rechtlichen Rahmenbedingungen für Telemedien und ist am **1. März 2007** in Kraft getreten.

Die Begriffe von Telediensten und Mediendiensten werden zusammengefasst, um die Anwendung des Gesetzes zu vereinfachen.

Vorher waren die Vorschriften auf
das Teledienstgesetz (TDG),
das Teledienstdatenschutzgesetz (TDDSG) und
den Mediendienststaatsvertrag (MDStV) verteilt;

diese wurden von dem Telemediengesetz abgelöst.

Quelle: http://www.informatik.uni-oldenburg.de/~iug11/rf/geschichte.html

Geschichte des Datenschutzes

2009

Da die Nutzung des Internets aber seit der ersten Veröffentlichung des Bundesdatenschutzgesetzes stark gestiegen ist, folgte ab 2009 eine ereignisreiche Zeit für den Datenschutz.

Der Deutsche Bundestag beschäftigte sich mit Änderungen für das Bundesdatenschutzgesetz und verfasste drei Novellen.

In der ersten Novelle wurden am 10. Juli der Anwendungsbereich und die ***Zulässigkeitsvoraussetzungen für das Scoring*** erweitert. Außerdem werden die Rechte von Betroffenen gestärkt, indem z.B. eine ***Auskunftspflicht seitens der Unternehmen*** besteht.

Die zweite Novelle vom 1. September befasst sich unter anderem mit einer ***Neuregelung des Arbeitnehmerdatenschutzes***, sowie mit den ***Zulässigkeits- und Transparenzanforderungen*** für personalisierte Werbung.

Inhalt der dritten Novelle ist die „***Umsetzung der EU-Richtlinien*** über Zahlungsdienste und Verbraucherkreditverträge".

Scoring
Der Begriff Scoring stammt aus dem Englischen; das Verb „to score" bedeutet dabei „Punkte erzielen".
Dies weist schon auf die Funktion des Score-Werts hin. Es handelt sich dabei um die Form eines Bonitätsindex.
Quelle: https://www.datenschutz-praxis.de/fachartikel/scoring-verfahren/

Quelle: http://www.informatik.uni-oldenburg.de/~iug11/rf/geschichte.html

Geschichte des Datenschutzes

2009 bis 2012

Der Deutsche Bundestag verfasste 2009 drei Novellen.

Die erste Novelle trat allerdings erst am 1. April 2010 und

die dritte Novelle erst am 11. Juli 2010 in Kraft.

Bei der zweiten Novelle existierte eine Übergangsfrist bis zum 1. Juli 2012.

Zusätzlich dazu wurde am 1. Dezember 2009 der Datenschutz in die Charta der Grundrechte der Europäischen Union aufgenommen.

Quelle: http://www.informatik.uni-oldenburg.de/~iug11/rf/geschichte.html

Geschichte des Datenschutzes

2012 bis 2014

2012 – ein Jahr der Entscheidungen im Datenschutz
Stagnation oder Aufbruch?
Das Jahr 2012 sollte grundlegende Entscheidungen für den Datenschutz bringen: Die Europäische Union plante neue Rechtsvorschriften, wobei zunächst noch vieles offen war: Sollte es eine Neufassung der EG-Datenschutzrichtlinie aus dem Jahr 1995 geben? Oder war an eine Verordnung gedacht?

EU-Verordnung statt EG-Richtlinie
Was schon seit Monaten gemunkelt wurde, wurde schließlich Realität:
Eine EU-Verordnung wird die bisherige EG-Datenschutzrichtlinie,
die noch aus dem Jahr 1995 stammt, im Wesentlichen ersetzen.

Entwurf 2012, wirksam ab 2014 oder noch später
Man konnte davon ausgehen, dass eine solche Verordnung im Januar 2012 zwar als Entwurf vorgelegt wird, jedoch frühestens Anfang 2014 in Kraft treten dürfte.

Inzwischen weiß man, dass dieser Zeitplan zu optimistisch war.
Die Beratungen werden dauern, und man wird der Praxis eine gewisse Umstellungszeit einräumen.

Wer sich darüber wundert, dass es 1995 „EG-Richtlinie“, aber jetzt „EU-Verordnung“ heißt:
Mit Wirkung vom 1.12.2009 – Inkrafttreten des Vertrags von Lissabon – trat die EU (Europäische Union) an die Stelle der EG (Europäische Gemeinschaft).

Es gibt also rechtlich gesehen schlicht keine EG mehr.

Geschichte des Datenschutzes

2012 bis 2014

EU-Verordnung statt EG-Richtlinie

Was schon seit Monaten gemunkelt wurde, wurde schließlich Realität:
Eine EU-Verordnung wird die bisherige EG-Datenschutzrichtlinie, die noch aus dem Jahr 1995 stammt, im Wesentlichen ersetzen.

Richtlinie oder Verordnung: Es werden nicht nur Begriffe ausgetauscht

Wer bei diesen Aktivitäten lediglich einen Austausch von Begriffen vermutet, täuscht sich.

Eine Richtlinie der Europäischen Union enthält zunächst nur Vorgaben für den nationalen Gesetzgeber, verbunden mit gewissen Spielräumen.

Es ist dann seine Sache, diese Vorgaben auf nationaler Ebene in Regelungen umzusetzen, die für das einzelne Unternehmen und den einzelnen Bürger verbindlich sind (siehe Art. 288 Abs. 3 des Vertrags über die Arbeitsweise der Europäischen Union).

Richtlinien führen zu großen Unterschieden in der Umsetzung

Diese Regelungstechnik hat in den letzten Jahren dazu geführt, dass die einzelnen Bestimmungen der Datenschutzrichtlinie in den Mitgliedstaaten zum Teil völlig unterschiedlich ausgelegt und angewandt wurden. Darauf hat die EU schon 2008 hingewiesen
(siehe http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf).

In Deutschland gibt es sogar innerhalb des Landes deutliche Anwendungsunterschiede.
Denn zwischen den 16 Landes-Datenschutzaufsichtsbehörden für die Privatwirtschaft liegen nicht nur geografische, sondern oft auch inhaltliche Distanzen.

Geschichte des Datenschutzes

2012 bis 2014

EU-Verordnung statt EG-Richtlinie
Wer bei diesen Aktivitäten lediglich einen Austausch von Begriffen vermutet, täuscht sich.

Eine Verordnung gilt unmittelbar

Eine Verordnung der Europäischen Union gilt entgegen der Richtlinie unmittelbar.
(Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union).

Sie bedarf also keiner Umsetzung in nationales Recht durch den nationalen Gesetzgeber, was schon einmal enorm Zeit bis zu ihrem Inkrafttreten spart.

Es wird weniger nationale Interpretationsspielräume geben
Zudem verringert dieses Vorgehen die Interpretationsspielräume erheblich.
Ganz beseitigt werden die Interpretationsspielräume allerdings nicht.

Das zeigt etwa die Diskussion um den Begriff „personenbezogene Daten“.
Er wird sehr unterschiedlich interpretiert. So betrachten manche das Bild eines Wohnhauses als personenbezogen, andere tun dies nicht.

Um eine einheitliche Interpretation zu gewährleisten, würde es also nicht ausreichen, einen solchen Begriff einfach aus der Richtlinie in eine Verordnung zu übernehmen.

Geschichte des Datenschutzes

2012 bis 2014

EU-Verordnung Interpretation

Um eine einheitliche Interpretation zu gewährleisten, würde es also nicht ausreichen,
einen solchen Begriff einfach aus der Richtlinie in eine Verordnung zu übernehmen.

Eine zentrale europäische Datenschutzaufsicht kommt

Um in dieser Hinsicht weiterzukommen, bedarf es einer zentralen Institution,
die für alle verbindlich sagt, „wo es langgeht“. Wie wichtig dies ist, zeigt sich gerade in Deutschland.
16 Landes-Datenschutzaufsichtsbehörden für die Privatwirtschaft bieten ein buntes Bild verschiedenster Rechtsauffassungen.

Was in Bayern erlaubt ist, ist es in Schleswig-Holstein noch lange nicht. Die ewige Diskussion um Google Analytics bietet insofern ein abschreckendes Beispiel. Als einheitliche Anlaufstelle für Unternehmen soll bei der EU-Kommission eine zentrale Aufsichtsbehörde geschaffen werden. Deren Aufgabe besteht dann darin, eine übereinstimmende Beurteilung des Datenschutzrechts in der EU zu gewährleisten.

Nationale Datenschutzaufsichten werden in erster Linie zu Beschwerdestellen für Bürger

Die **nationalen Aufsichtsbehörden** werden künftig vor allem eine **Anlaufstelle für Bürger** sein, **die sich wegen Datenschutzverstößen beschweren wollen**. Bei der rechtlichen Beurteilung Rechtskompass
werden die nationalen Aufsichtsbehörden die rechtlichen Einschätzungen der zentralen Aufsichtsbehörde zu beachten haben.

Geschichte des Datenschutzes

2012 bis 2015

EU-Verordnung Interpretation

Um eine einheitliche Interpretation zu gewährleisten, würde es also nicht ausreichen, einen solchen Begriff einfach aus der Richtlinie in eine Verordnung zu übernehmen.

Vorschlag der Europäischen Kommission vom 25. Januar 2012:
Grundlage für die weiteren Verhandlungen

Abänderungen durch das Europäische Parlament am 12. März 2014:
über 200 Vorschläge für Änderungen

Beschluss des Rats der Innen- und Justizminister 15. Juni 2015:
gemeinsamer Standpunkt gegenüber dem Vorschlag der EU-Kommission, Billigung einer „allgemeinen Ausrichtung“

Handlungsbedarf zur EU-DSGVO (DatenSchutzGrundVerOrdnung)

Am 4. Mai 2016, und damit deutlich früher als angekündigt, wurde die EU-Datenschutz-Grundverordnung (EU-DSGVO) im Amtsblatt der Europäischen Union veröffentlicht.

Art. 99 Abs. 2 der Verordnung lautet: „**Sie gilt ab dem 25. Mai 2018**.“

In der knappen Zeit bis dahin müssen Unternehmen

- interne Prozesse überprüfen,
- Verträge nachverhandeln und
- möglicherweise auch Einwilligungserklärungen anpassen.

Handlungsbedarf zur EU-DSGVO (DatenSchutzGrundVerOrdnung)

Bislang beruht das europäische Datenschutzrecht auf einer Richtlinie aus dem Jahr 1995 (Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr).

Diese Richtlinie ist die Basis für ein europaweites Datenschutzniveau mit den Kernelementen

- Verbot mit Erlaubnisvorbehalt,
- Zweckbindung,
- Gewährleistung von Betroffenenrechten und
- Unabhängigkeit der Aufsichtsbehörden.

Diese Grundsätze bleiben in der Datenschutz-Grundverordnung erhalten.
Sie werden jedoch teilweise **detaillierter geregelt**.

Handlungsbedarf zur EU-DSGVO

Grundlagen für die Rechtmäßigkeit der Datenverarbeitung

Wie bisher benötigt ein Unternehmen oder eine Behörde eine Rechtsgrundlage, um personenbezogene Daten verarbeiten zu können (Art. 6 DSGVO).
Diese Rechtsgrundlage kann sein

- eine gesetzliche Regelung oder
- die Einwilligung des Betroffenen

Unternehmen können wie bisher die Wahrung
eigener berechtigter Interessen als Grundlage heranziehen.

Diese Interessen müssen sie mit den Interessen der betroffenen Person abwägen.

Handlungsbedarf zur EU-DSGVO

Anforderungen an Einwilligungen

Welche Anforderungen gelten nun für eine Einwilligung (Art. 7 DSGVO)?

Der Erwägungsgrund 32 der Grundverordnung gibt dazu Hinweise:

- Sie ist auch elektronisch möglich.
- Sie muss klar den Zweck der Datenverarbeitung erkennen lassen.
- Sie muss für die betroffene Person leicht verständlich formuliert sein.

Handlungsbedarf zur EU-DSGVO

Zweckbindung

Unabhängig davon, welche Rechtmäßigkeitsgrundlage greift:

Bei der Erhebung muss der Zweck der Datenverarbeitung festgelegt sein.

Und der Betroffene muss den Zweck erkennen können.

Zweckänderungen sind später nur in sehr engen Grenzen möglich.

Handlungsbedarf zur EU-DSGVO

Betroffenenrechte I.

Weiterhin ist die betroffene Person über die
erstmalige Speicherung ihrer Daten zu informieren (Artt. 13 und 14 DSGVO).

Diese Informationspflicht umfasst nun aber wesentlich
mehr Punkte als § 33 im Bundesdatenschutzgesetz (BDSG).

Neue Anforderungen sind u.a.

- die Angabe der voraussichtlichen Dauer der Speicherung,
- das Widerspruchsrecht sowie ggf. die Folgen eines Widerspruchs und
- die Darlegung der Abwägungsgründe, sofern eine Abwägung stattfindet.

Handlungsbedarf zur EU-DSGVO

Betroffenenrechte II.

Die Grundverordnung sieht wie bisher

Auskunftspflichten des Verantwortlichen (= „verantwortliche Stelle“ im BDSG) gegenüber der betroffenen Person vor.

Neu hinzu kommen die – breit in der Öffentlichkeit diskutierten – Regelungen zu

- einem Anspruch auf Datenportabilität und
- einem „Recht auf Vergessenwerden“.

Handlungsbedarf zur EU-DSGVO

Dokumentationspflichten

Das bisherige interne Verfahrensverzeichnis wird durch ein **Verzeichnis der Verarbeitungstätigkeiten** (Art. 30 DSGVO) ersetzt. Im Gegensatz zur derzeitigen Regelung müssen auch Auftragsverarbeiter (bisher „Auftragsdatenverarbeiter“) eines anlegen. Ein Jedermannsverzeichnis, d.h. die Pflicht, es jedermann auf Verlangen auszuhändigen, besteht nicht mehr. Unternehmen müssen das Verzeichnis aber auf Anforderung der Aufsichtsbehörde vorlegen. Das Verzeichnis soll wesentliche Informationen zusammenfassen, u.a.

- Zweck der Verarbeitung,
- Löschfristen,
- Empfänger, aber auch
- Abwägungsgründe sowie
- technische und organisatorischen Schutzmaßnahmen.

Erleichterungen in diesem Punkt sind für Unternehmen mit weniger als 250 Mitarbeitern möglich.

Handlungsbedarf zur EU-DSGVO

Sicherheit der Verarbeitung

Sowohl der Verantwortliche als auch der Auftragsverarbeiter müssen
technische und organisatorische Maßnahmen treffen,
um ein angemessenes Schutzniveau zu gewährleisten
(Art. 32 DSGVO).

Die Vorgaben hierzu ersetzen
die aus der Anlage zu § 9 BDSG
bekannten Vorgaben der IT-Sicherheit.

Handlungsbedarf zur EU-DSGVO

Data protection by design und by default

Laut Artikel 23 der Verordnung muss Datenschutz künftig direkt in Prozesse, Systeme und Produkte eingebaut werden.

Technisch voreingestellte Standards und Datenminimierung über die Voreinstellungen werden an Bedeutung gewinnen
(Art. 25 DSGVO).

Details hierzu können europäische Institutionen noch vorgeben.

Inwieweit sich der im Januar 2015 veröffentlichte Vorschlag der ENISA (European Union Agency for Network and Information Security) vom Dezember 2014 zu privacy und data protection by design unmittelbar auswirken wird, ist derzeit offen

http://t1p.de/enisaprotection-by-design

https://www.heise.de/newsticker/meldung/Privacy-by-Design-EU-Sicherheitsbehoerde-legt-Empfehlungen-vor-2517870.html

Handlungsbedarf zur EU-DSGVO

Datenschutz-Folgenabschätzung

Bislang musste der Datenschutzbeauftragte bei bestimmten Konstellationen in Form einer Vorabkontrolle die Folgen einer Datenverarbeitung für die Rechte und Freiheiten der betroffenen Person prüfen.

Diese Prüfung, nun als **Datenschutz-Folgenabschätzung** bezeichnet, muss der Verantwortliche künftig häufiger durchführen (Art. 35 DSGVO).

Wichtig!
Generell werden die Risikobetrachtung und die daraus abzuleitenden Maßnahmen eine der Kernaufgaben einer künftigen Datenschutzorganisation.

Handlungsbedarf zur EU-DSGVO

Konsultation der Aufsichtsbehörde

In den Fällen, in denen die Schutzmaßnahmen zur Eindämmung eines Risikos nicht ausreichen, konsultiert der Verantwortliche seine zuständige Aufsichtsbehörde (Art. 36 DSGVO).

Sie gibt dann innerhalb einer festgelegten Frist Hinweise oder eine Stellungnahme ab.

Handlungsbedarf zur EU-DSGVO

Meldepflicht bei Datenpannen

Die Grundverordnung weitet die Meldepflicht bei Datenpannen aus:

- Es gibt keine Beschränkung auf bestimmte Datenarten mehr.

- Zudem werden auch öffentliche Stellen von der Meldepflicht an die zuständige Aufsichtsbehörde und an die betroffene Person umfasst.

Handlungsbedarf zur EU-DSGVO

Unternehmensgruppen

Es gibt nach wie vor kein Konzernprivileg im Datenschutzrecht.

Doch wird die Datenweitergabe innerhalb einer Unternehmensgruppe als berechtigtes Interesse anerkannt.

Handlungsbedarf zur EU-DSGVO

Auftragsverarbeitung

Die Grundprinzipien der Auftragsdatenverarbeitung bleiben erhalten:

- Der Auftraggeber bleibt wie bisher verantwortlich.
- Eine ausdrückliche Rechtmäßigkeitsgrundlage für die Datenweitergabe ist weiterhin nicht erforderlich – mit dem Dienstleister sind aber bestimmte inhaltliche Punkte zu regeln (Art. 28 DSGVO).
- Beibehalten wird auch, dass der Auftraggeber nicht vor Ort beim Auftragnehmer erscheinen muss.

  Um einen Nachweis zu erhalten, dass der Auftragnehmer seine Pflichten erfüllt und die vereinbarten technischen und organisatorischen Maßnahmen einhält, lassen sich wie bisher Zertifikate oder genehmigte Verhaltensregeln heranziehen.

Handlungsbedarf zur EU-DSGVO

Haftung bei der Auftragsverarbeitung

Neu ist, dass Auftraggeber und Auftragnehmer gemeinsam gegenüber der betroffenen Person für einen Datenschutzverstoß einstehen müssen, es sei denn, einer von beiden kann sich vollständig entlasten (Art. 82 DSGVO).

- Aus Sicht des Auftraggebers ändert sich nichts – war er doch bisher schon als „verantwortliche Stelle“ für die Einhaltung der Datenschutzanforderungen gegenüber Betroffenem im Haftungsrisiko.

- Für den datenverarbeitenden Dienstleister erhöht sich jedoch das Risiko. Denn nun könnten Geschädigte auch ihn in Anspruch nehmen. Und er trägt auch das Risiko, sich nicht entlasten zu können.

Handlungsbedarf zur EU-DSGVO

Zertifizierungen und genehmigte Verhaltensregeln

An zahlreichen Stellen fordert die Grundverordnung Nachweise dafür, dass Unternehmen oder Behörden die erforderlichen Schutzmaßnahmen einhalten:

Sei es für die Datenverarbeitung (Art. 24 DSGVO),
bei der Auftragsverarbeitung (Art. 28 DSGVO) oder
bei den technischen Anforderungen an Schutzmaßnahmen (Art. 25, 32 DSGVO).

Die Verordnung regelt auch die Verfahren zu
genehmigten Verhaltensregeln (Art. 40 DSGVO) und
Zertifizierungen (Art. 42 DSGVO),
die als Nachweise dienen können.

Handlungsbedarf zur EU-DSGVO

Aufsichtsbehörden

Bei grenzüberschreitenden Fragestellungen wird es eine einzige federführende Aufsichtsbehörde geben („One-Stop-Shop“).

Als **One-Stop-Shop** wird in der Wirtschaft wie auch in der öffentlichen Verwaltung die Möglichkeit bezeichnet, alle notwendigen bürokratischen Schritte, die zur Erreichung eines Zieles führen, an einer einzigen Stelle durchzuführen. Hierzu zählen Unternehmensgründungen, bürokratische Alltagsaufgaben, Finanzaufgaben, Steuererklärungen, etc. Im Rahmen der europäischen Fusionskontrolle bedeutet One-Stop-Shop, dass lediglich die Europäische Kommission ein Prüfungsrecht hat und der Zusammenschluss nicht daneben auch von Mitgliedsstaaten überprüft werden kann.

Quelle: https://de.wikipedia.org/wiki/One-Stop-Shop

Ein Kohärenzverfahren soll eine inhaltliche Abstimmung zwischen den beteiligten Aufsichtsbehörden garantieren.

Handlungsbedarf zur EU-DSGVO

Datenschutzbeauftragter

Die EU-DSGVO führt europaweit den behördlichen Datenschutzbeauftragten ein.

Für Unternehmen gibt es Sonderregelungen.

Darüber hinaus können die Mitgliedstaaten über eine Öffnungsklausel die Bestellpflichten auf nationaler Ebene regeln.

Folgt man den Aussagen der politischen Repräsentanten aus den letzten Jahren, so wird sich in Deutschland am derzeitigen Status des Datenschutzbeauftragten nichts ändern.

Weisungsfreiheit, Benachteiligungsverbot und Anspruch auf angemessene Ausstattung sind die Kernelemente des betrieblichen Datenschutzbeauftragten, die in Deutschland höchstwahrscheinlich erhalten bleiben.

Handlungsbedarf zur EU-DSGVO

Öffnungsklauseln

Öffnungsklauseln wie beim Datenschutzbeauftragten geben den Mitgliedstaaten die Möglichkeit, auf nationaler Ebene Vorgaben zu machen.

Das betrifft z.B. auch
die Verringerung des Mindestalters bei Minderjährigen (Art. 8 DSGVO) oder
den Beschäftigtendatenschutz (Art. 88 DSGVO).

In diesem Rahmen wird sich der deutsche Gesetzgeber auch entscheiden, ob er das BDSG ganz aufhebt oder Teile daraus für die Regelungsbereiche, die dem nationalen Gesetzgeber zugewiesen wird, verwendet.

Was passiert nach dem 25. Mai 2018, wenn nichts passiert?

Verschärfte Sanktionen

Waren bei Datenschutzverstößen nach dem BDSG
bisher Bußgelder bis zur Höhe von 50.000 oder 300.000 Euro vorgesehen,

erhöht sich der Bußgeldrahmen
bei Verstößen gegen die meisten der hier dargestellten Pflichten
auf 2 % des weltweiten Jahresumsatzes bzw.
auf Beträge bis 10 Mio. Euro

– je nachdem, welcher Betrag höher ist (Art. 83 DSGVO).

Bei schwerwiegenden Verstößen wie einer Weitergabe in ein Drittland oder bei Verstößen gegen Anordnungen der Aufsichtsbehörden
erhöhen sich diese Zahlen auf 4 % bzw. 20 Mio. Euro.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

- interne Prozesse überprüfen,
- Verträge nachverhandeln und
- möglicherweise auch Einwilligungserklärungen anpassen.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Zulässigkeit der Verarbeitung

Frage	ok	Maßnahme
Ist für jede Bearbeitung personenbezogener Daten festgelegt, zu welchem Zweck sie erfolgt bzw. auf Grund welcher Rechtsgrundlage?		Definieren Sie für jedes einzelne Verfahren der personenbezogenen Datenverarbeitung den Zweck.
Wurde für alle personenbezogenen Daten die Zulässigkeit der Erhebung, Verarbeitung und des Nutzens geprüft?		Prüfen Sie, ob die DSGVO die Verarbeitung der personenbezogenen Daten erlaubt bzw. dazu verpflichtet oder eine Zulässigkeit im Sinne der Verordnung vorliegt.
Wird darauf geachtet, dass bei einer Einwilligung der Betroffenen diese auch schriftlich erfolgt?		Überprüfen Sie die Einwilligungserklärung von Betroffenen hinsichtlich der Wirksamkeit.
Wird bei der Erhebung der Daten sowie an anderen geeigneten Stellen auf die automatisierte Verarbeitung hingewiesen, um den Betroffenen Art und Umfang der Verarbeitung ihrer personenbezogenen Daten so transparent wie möglich zu machen?		Stellen Sie sicher, dass bei der Datenerhebung die Betroffenen hinsichtlich des Umfangs der Datenverarbeitung und ihrer Rechte ausreichend informiert werden.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Mitarbeiterschulung und Datenschutzverpflichtung

Frage	ok	Maßnahme
Sind alle Mitarbeiter/innen, die personenbezogene Daten bearbeiten, auf das Datengeheimnis verpflichtet?		Legen Sie ein Verfahren fest, dass Mitarbeiter, die personenbezogene Daten verarbeiten, schon bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet werden.
Wurde die Datenschutzverpflichtung dokumentiert?		Definieren Sie die Form der Datenschutzverpflichtung von Mitarbeitern, die verpflichtet werden (schriftlich mit Unterschrift des Mitarbeiters).
Wurden alle Mitarbeiter/innen durch Schulungen ausreichend sensibilisiert?		Erstellen Sie einen Schulungsplan für alle Mitarbeiter, die personenbezogene Daten verarbeiten und setzen Sie den Schulungsplan um. Informieren Sie die Mitarbeiter regelmäßig zum Thema Datenschutz.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Verfahrensverzeichnisse

Frage	ok	Maßnahme
Liegen aktuelle interne Verfahrensübersichten bzw. ein Verfahrensverzeichnis vor und werden diese bei Veränderungen zeitnah gepflegt?		Die geforderten Angaben für das Verfahrensverzeichnis entnehmen Sie der DSGVO. Erstellen Sie zusätzlich ein Verfahrensverzeichnis für "Jedermann".
Sind die Angaben gemäß DSGVO im Verfahrensverzeichnis in ausreichender Genauigkeit dargestellt?		Überprüfen Sie, ob anhand des erstellten Verfahrensverzeichnisses eine Bewertung der datenschutzgerechten Verarbeitung der Daten möglich ist.
Sind die Angaben im "Verfahrensverzeichnis für Jedermann" ausreichend beschrieben?		Überprüfen Sie, ob alle durch den Gesetzgeber geforderten Angaben im "Verfahrensverzeichnis für Jedermann" in der notwendigen Tiefe vorhanden sind. Falls nicht, sollten Sie das Verzeichnis überarbeiten.
Gibt es Vorgaben, die sicherstellen, dass das Verfahrensverzeichnis aktuell gehalten wird?		Etablieren Sie in der Organisation Ihres Unternehmens einen Prozess, der sicherstellt, dass neue oder geänderte Verfahren an Sie gemeldet werden.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Technische und organisatorische Maßnahmen

Frage	ok	Maßnahme
Gibt es eine Dokumentation aller sicherheitsrelevanten Maßnahmen?		Dokumentieren Sie getroffene Maßnahmen zur IT-Sicherheit (IT-Sicherheitskonzept)
Zutrittskontrolle:		
Ist festgelegt, welche Personen Zutritt zu Datenverarbeitungsanlagen (Server-Räume etc.) haben?		Die IT muss eine Liste der Mitarbeiter zur Verfügung stellen, die Zutritt zu den Datenverarbeitungsanlagen haben. Überprüfen Sie die Verpflichtung dieser Mitarbeiter.
Gibt es Regelungen für Externe (Wartungspersonal, Reinigungspersonal, Dienstleister etc.)?		Überprüfen Sie, ob es datenschutzgerechte Regelung für den Zutritt von externen Personen gibt.
Sind die Räume mit Sicherheitsschlössern bzw. elektronischen Zugangssystemen gesichert?		Überprüfen Sie die Absicherung der Zutrittssicherheit der Räume, in denen sich Datenverarbeitungssysteme befinden.
Sind die Außenfenster entsprechend gesichert?		Überprüfen Sie die physische Absicherung der Räume, in denen sich Systeme mit personenbezogenen Daten befinden.
Werden die eingeführten Sicherheitsmaßnahmen regelmäßig überprüft?		Erstellen Sie eine Richtlinie und eine Checkliste, mit denen Sie eine regelmäßige Überprüfung der IT-Sicherheitsmaßnahmen durchführen und dokumentieren.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Technische und organisatorische Maßnahmen

Frage	ok	Maßnahme
Zugangskontrolle:		
Muss sich jeder Benutzer durch Eingabe einer Benutzerkennung und Passwort oder durch andere technische Mittel (Chipkarte) identifizieren?		Stellen Sie durch Richtlinien, Vorgaben und technische Maßnahmen sicher, dass nur berechtigte Personen Zugang zu Systemen, mit denen personenbezogene Daten verarbeitet werden, haben.
Werden Bildschirmschoner eingesetzt, die sich automatisch nach einer definierten Zeit einschalten und nur nach Eingabe eines Passwortes wieder ausschalten?		Stellen Sie sicher, dass personenbezogene Daten nicht zufällig bekannt werden.
Gibt es eine Regelung zur Passwortvergabe (Mindestlänge, Trivialkennwort, Sonderzeichen etc.)?		Durch eine Regelung ist sicherzustellen, dass Passwörter die notwendige Stärke haben.
Gibt es technische oder organisatorische Maßnahmen zur erzwungenen, regelmäßigen Änderung des Passwortes?		Stellen Sie sicher, dass Passwörter regelmäßig geändert werden müssen. Die Sequenz der Änderungen muss sich nach der Sensibilität der Daten richten.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Technische und organisatorische Maßnahmen

Frage	ok	Maßnahme
Zugriffskontrolle:		
Existiert ein Konzept zur Vergabe von Zugriffsrechten?		Erstellen Sie ein Konzept und die notwendigen Verfahrensrichtlinien, die sicherstellen, dass nur berechtigte Mitarbeiter Zugriff auf personenbezogene Daten haben.
Werden Zugriffsrechte regelmäßig überprüft?		Etablieren Sie einen Prozess, der eine regelmäßige Überprüfung der Zugriffsberechtigung der einzelnen Mitarbeiter sicherstellt.
Existiert ein Verfahren, das sicherstellt, dass bei ausscheidenden Mitarbeitern die Zugriffsrechte deaktiviert werden?		Erstellen Sie ein Konzept und die notwendigen Verfahren, um sicherzustellen, dass Zugriffsrechte bei Änderung der Tätigkeit oder Ausscheiden von Mitarbeitern zeitnah angepasst oder gelöscht werden.
Ist bei Wartung oder Fernwartung von Systemen in Ihrem Unternehmen sichergestellt, dass die externen Dienstleister keinen Zugriff auf personenbezogene Daten haben?		Stellen Sie sicher, dass externe Personen, die eine Wartung von Systemen durchführen, keinen Zugriff auf personenbezogene Daten erhalten.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Technische und organisatorische Maßnahmen

Weitergabekontrolle:		
Frage	ok	Maßnahme
Gibt es Regelungen, welche Daten über das Internet übertragen werden dürfen?		Wirken Sie auf eine Regelung hin, die die datenschutzrechtlichen Grundsätze bei der dienstlich/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz beinhaltet.
Werden die personenbezogenen Daten bei der Übertragung (z. B. E-Mail) verschlüsselt?		Stellen Sie sicher, dass keine personenbezogenen Daten unverschlüsselt über das Internet transportiert werden.
Werden bei Übertragung von personenbezogenen Daten über ein WLAN die notwendigen Sicherheitsmaßnahmen eingesetzt?		Wirken Sie darauf hin, dass durch technische Maßnahmen (Verschlüsselung, Authentisierung) nur eine gesicherte Übertragung von personenbezogenen Daten über WLAN-Verbindungen erfolgt.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Technische und organisatorische Maßnahmen

Eingabekontrolle:		
Frage	ok	Maßnahme
Sind die für die Eingabekontrolle verantwortlichen Personen festgelegt?		Legen Sie durch organisatorische Regelungen fest, welche Daten zur Eingabekontrolle protokolliert werden und wer die Protokolldateien auswerten darf.
Sind die Personen, die für die Eingaben verantwortlich sind, organisatorisch festgelegt?		Wirken Sie darauf hin, dass durch entsprechende organisatorische Anweisungen nur berechtigte Personen personenbezogene Daten erfassen und verarbeiten.
Gibt es Anweisungen für die Datenerfassung und den Verbleib von Eingabebelegen?		Wirken Sie darauf hin, dass durch entsprechende organisatorische Regelungen festgelegt wird, wie bei der Datenerfassung verfahren wird und wie mit Belegen mit personenbezogene Daten hinsichtlich Lagerung, Vernichtung etc. verfahren wird.
Werden Log-Dateien regelmäßig ausgewertet?		Stellen Sie sicher, dass personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, ausschließlich für diese Zwecke verwendet werden und dass die Personen, die die Log-Files auswerten, auf das Datengeheimnis verpflichtet wurden.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Technische und organisatorische Maßnahmen

Auftragskontrolle:		
Frage	ok	Maßnahme
Werden bei der Verarbeitung personenbezogener Daten durch Dritte entsprechende vertragliche Regelungen zum Datenschutz getroffen?		Wirken Sie darauf hin, dass bei der Verarbeitung von personenbezogenen Daten durch externe Firmen die Regelungen der DSGVO vertraglich vereinbart werden.
Werden beim Auftragnehmer regelmäßig Kontrollen (Besichtigung der Räumlichkeiten, der Datenverarbeitung, Sicherheitskonzept, Verpflichtung der Mitarbeiter) durchgeführt?		Wirken Sie darauf hin, dass bei der Verarbeitung von personenbezogenen Daten durch Externe eine vertragliche Vereinbarung getroffen wird, die Ihnen eine Kontrolle der getroffenen Datenschutzmaßnahmen erlaubt.
Wird sichergestellt, dass bei externer Vernichtung von Datenträgern dies auch ordnungsgemäß durchgeführt wird?		Wirken Sie darauf hin, dass bei Verträgen zur Vernichtung von Akten oder elektronischen Datenträgern eine datenschutzgerechte Entsorgung gesichert ist und sorgen Sie für Kontrollmöglichkeiten.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Technische und organisatorische Maßnahmen

Verfügbarkeitskontrolle:		
Frage	ok	Maßnahme
Gibt es ein detailliertes Datensicherungskonzept?		Wirken Sie darauf hin, dass die IT in Ihrem Unternehmen ein Datensicherungskonzept hat, in dem die Wiederherstellung von gelöschten oder zerstörten Daten sichergestellt wird.
Sind die Zuständigkeiten und Verantwortlichkeiten für die Datensicherung allen Beteiligten bekannt und bewusst?		Überprüfen Sie, ob durch Regelungen sichergestellt wird, wer für die Datensicherung im Unternehmen verantwortlich ist.
Wird regelmäßig überprüft, ob ein Wiedereinspielen der gesicherten Daten möglich ist?		Überprüfen Sie, ob durch regelmäßige Prüfung auch sichergestellt wird, dass gesicherte Daten wiederhergestellt werden können.
Ist sichergestellt, dass nicht genutzte Datenträger (Archiv) an einem sicheren Ort gelagert werden?		Überprüfen Sie, ob die Lagerung von Datenträgern und Akten auch datenschutzgerecht erfolgt und kein unberechtigter Zugriff auf die Archivobjekte ermöglicht wird.

Empfohlene Maßnahmen

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

Technische und organisatorische Maßnahmen

Zwecktrennungsgebot:		
Frage	ok	Maßnahme
Ist sichergestellt, dass personenbezogene Daten verschiedener speichernder Stellen gegeneinander durch logische (Berechtigungskonzept) oder physikalische (unterschiedliche Systeme/Datenbanken) Trennung abgeschottet sind?		Überprüfen Sie, ob durch technische Maßnahmen und/oder ein Berechtigungskonzept sichergestellt ist, dass personenbezogene Daten, welche zu unterschiedlichen Zwecken erfasst wurden, auch getrennt verarbeitet werden.

Empfohlene Maßnahmen

Laut Artikel 23 der Verordnung muss Datenschutz künftig direkt in Prozesse, Systeme und Produkte eingebaut werden.

Jetzt handeln - Noch ist genügend Zeit !

Geschäftsprozesse aus Sicht der EU-DSGVO beleuchten

- interne Prozesse überprüfen,
- Verträge nachverhandeln und
- möglicherweise auch Einwilligungserklärungen anpassen.

Datenschutz-Folgenabschätzung und
Datenschutz-Maßnahmen in das Qualitäts-Management-System einbinden

→ Wirtschaftliche Einhaltung der EU-DSGVO ←

→ Wirtschaftliche Einhaltung der EU-DSGVO ←

Blickhan Datentechnik.de

Beratung zur wirtschaftlichen Einhaltung von EU-Richtlinien und Gesetzen

Mein Support – Ihr Nutzen:

→ Datenschutz@Blickhan.de

- ✓ Individuelle Beratung zur wirtschaftlichen Einhaltung der EU-DSGVO
- ✓ Externer Datenschutzbeauftragter

- ✓ Aktuelle Informationen und Fragen zum Datenschutz

- ✓ Datenschutz-Dialog in der Metropolregion Frankfurt Rhein-Main-Neckar
- ✓ Beratung für verfahrensrechtliche und verfahrenstechnische Maßnahmen in kleinen praxisorientierten Gruppen