DSGVO

Fünf Buchstaben, viele offene Fragen

life PR

DSGVO – FÜNF BUCHSTABEN, VIELE OFFENE FRAGEN

Seit etwa zwei Jahren geistert ein Begriff durch die europäischen Medien und mit jedem Tag, der sich dem 25. Mai 2018 nähert, steigt die Verunsicherung auch in IT- und Marketingabteilungen deutscher Unternehmen, wenn die Sprache zwangsläufig auf die mit diesem Datum verpflichtend anzuwendende Datenschutz-Grundverordnung (DSGVO) kommt.

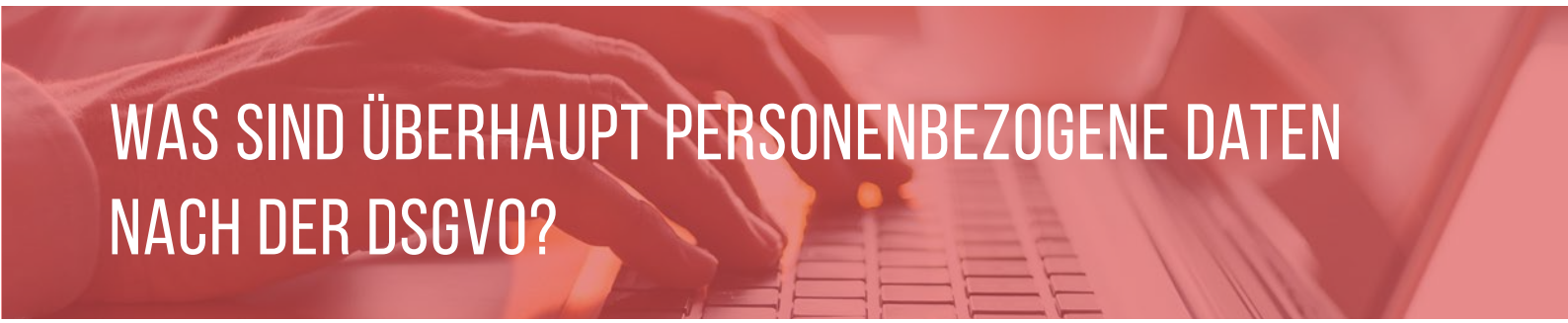
An dieser Stelle möchten wir Ihnen einen Überblick darüber verschaffen, welche Neuerungen im Datenschutz mit der Verordnung der Europäischen Union verbunden sind, inwieweit diese von der aktuellen Praxis im Rahmen des Bundesdatenschutzgesetzes (BDSG) abweichen und welche Auswirkungen auf Ihren Unternehmensalltag die neue Verordnung haben kann.

WIE IST DER STATUS QUO IN FRAGEN DATENSCHUTZ?

- Seit 1995 gilt für Europa die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
- Als Richtlinie obliegt es jedem Mitgliedsstaat, diese in nationales Recht umzusetzen. Dies geschah in Deutschland im Rahmen des Bundesdatenschutzgesetzes.
- Weite Teile der neuen Datenschutz-Grundverordnung finden im deutschen Recht durch das Bundesdatenschutzgesetz in zumindest grundlegender Form bereits seit Jahren Anwendung.

WIESO DIE NEUE DATENSCHUTZ-GRUNDVERORDNUNG?

- Hauptanliegen der DSGVO ist eine Vereinheitlichung der Bestimmungen zum Datenschutz in ganz Europa und eine Harmonisierung der nationalen Bedingungen.
- Als Verordnung muss die DSGVO von den Mitgliedsstaaten übernommen und erfüllt werden. Eine individuelle nationale Umsetzung findet zumindest in den Grundzügen der Verordnung nicht mehr statt.
- Die DSGVO soll insgesamt den Schutz vor Missbrauch personenbezogener Daten und damit die Persönlichkeitsrechte des Verbrauchers stärken.



WAS SIND ÜBERHAUPT PERSONENBEZOGENE DATEN NACH DER DSGVO?

- Personenbezogene Daten im Sinne der DSGVO sind alle Daten, die sich auf eine bekannte („identifizierte“) Person beziehen oder aber eine Identifizierung einer Person zulassen.

Daten, die eine **direkte Identifikation einer Person** zulassen sind zum Beispiel:

- Name
- Adresse
- Telefonnummer
- E-Mail-Adresse
- Geburtsdatum
- Bild
- Kontodaten
- usw.

Die **Möglichkeit zur indirekten Identifizierung** ergibt sich dagegen bereits aus Daten wie:

- Nutzername
- Profilbild
- IP-Adresse
- Cookie-ID

- Von der DSGVO betroffene Daten fallen im allgemeinen Geschäftsbetrieb im Kundenkontakt an. Sie werden zum Beispiel im Rahmen von Bestellvorgängen erhoben, können aber auch gezielt im Rahmen des Marketings zu vielfältigen Zwecken erhoben werden.
- Die Erhebung, Sammlung, Speicherung, Auswertung und Weiterverwendung von personenbezogenen Daten wird bis heute in weiten Teilen bereits durch das Bundesdatenschutzgesetz geregelt.

FÜR WEN GILT DIE DSGVO?

- Grundsätzlich gilt die DSGVO für jeden, der personenbezogene Daten ganz oder teilweise automatisiert verarbeitet oder nicht-automatisiert erhebt und speichert.
- Die DSGVO gilt gleichermaßen für Personen, Körperschaften und Institutionen jeder Art und Größe.
- Die DSGVO gilt für Unternehmen und Organisationen in den 28 Staaten der EU sowie für solche außerhalb der EU, sofern deren Datenverarbeitung EU-Bürger betrifft.
- Ausgenommen ist die Datenverarbeitung zum Schutz der Grundrechte und Grundfreiheiten, zum Beispiel in Fragen der nationalen Sicherheit.
- Ebenfalls ausgenommen ist die Datenerhebung und Datenverarbeitung zu rein persönlichen oder familiären Zwecken ohne beruflichen Bezug oder wirtschaftliches Interesse.

AB WANN GILT DIE DSGVO?

- In Kraft getreten ist die DSGVO bereits am 24. Mai 2016.
- Anzuwenden sind die Vorschriften der DSGVO konkret ab dem 25. Mai 2018.

WELCHE AUFLAGEN DER DSGVO WERDEN BEREITS VOM BUNDESDATENSCHUTZGESETZ (BDSG) ERFÜLLT?

- Schon das BDSG hat die Zielsetzung, das informationelle Selbstbestimmungsrecht als Teil der Grundrechte zu achten und zu stärken.
- Grundsätzlich erlaubt schon das BDSG die Erhebung, Verarbeitung und Speicherung personenbezogener Daten nur unter konkreten Auflagen.
- BDSG und DSGVO erklären die Einwilligung des Betroffenen als unverzichtbare Grundvoraussetzung für die Datenerhebung.
- Bereits das BDSG verpflichtet Unternehmen, welche sich in der Hauptsache mit der Datenerhebung und Datenverarbeitung befassen, einen betrieblichen Datenschutzbeauftragten zu beschäftigen.
- Die Datenverarbeitung ist bereits laut BDSG ausschließlich zweckgebunden gestattet.

WO LIEGEN DIE NEUERUNGEN DER DSGVO?

- Die DSGVO definiert im Detail den Begriff der personenbezogenen Daten.
- Dem Betroffenen steht nicht nur das Recht zu, alleine durch seine Zustimmung über eine Datenerhebung und Datenverarbeitung zu entscheiden, er hat auch ein detailliert geregeltes Auskunftsrecht.
- Auf Verlangen müssen dem Betroffenen detaillierte Informationen zu den verarbeiteten personenbezogenen Daten übermittelt werden. Diese beinhalten:
    - die grundlegende Information, ob Daten erhoben wurden
    - die Verarbeitungszwecke
    - Kategorien der personenbezogenen Daten
    - die Empfänger oder Kategorien von Empfängern, denen Daten offengelegt wurden oder noch offengelegt werden sollen
    - die geplante Dauer der Speicherung
    - Informationen über die Herkunft der Daten
    - Informationen über automatisierte Auswertung der Daten im Sinne eines Profilings, dessen Logik und potentielle Auswirkungen für die betroffene Person

- Der Betroffene hat ein Anrecht auf eine kostenlose Kopie der über ihn vorhandenen Daten. Für weitere Kopien kann ein Entgelt erhoben werden.
- Der Betroffene hat ein Recht auf Löschung oder Berichtigung der gespeicherten Daten.
- Der Betroffene hat das „Recht auf Vergessenwerden“: Personenbezogene Daten müssen vollständig gelöscht werden, wenn
    - sie für den Zweck, zu dem sie erhoben wurden nicht mehr nötig sind,
    - der Betroffene eine Einwilligung widerruft,
    - der Betroffene Widerspruch gegen die Verarbeitung einlegt,
    - die Daten unrechtmäßig erhoben oder verarbeitet wurden.

- Die von der DSGVO bei Zuwiderhandlung vorgesehenen Bußgelder sind deutlich höher als bisher vom BDSG vorgesehen. In Einzelfällen können diese bis 20 Mio. Euro oder bis zu vier Prozent des weltweiten Jahresumsatzes des sanktionierten Unternehmens betragen. Vom BDSG wurden Bußgelder von maximal 300.000 Euro vorgesehen.
- Der Geltungsbereich der DSGVO ist deutlich größer als der des BDSG. Ausschlaggebend ist letztlich der Standort der Person, zu der Daten verarbeitet werden, auch wenn das verarbeitende Unternehmen selber nicht in der EU niedergelassen ist.
- Einzelne Unternehmen und Institutionen sind durch die DSGVO zu einer Datenschutz-Folgeabschätzung verpflichtet, in deren Rahmen das individuelle Risiko der Verletzung der Datenschutzrichtlinien bewertet und über geeignete Schutzmaßnahmen Rechenschaft abgelegt werden muss.
- Kommt es zu einer Verletzung der Datenschutzvorschriften sind die Verantwortlichen verpflichtet, Betroffene binnen 72 Stunden über Art und Umfang der Verletzung zu informieren.

WER BENÖTIGT EINEN DATENSCHUTZBEAUFTRAGTEN UND WAS SIND DESSEN AUFGABEN?

- Die Benennung eines Datenschutzbeauftragten ist **nicht von der Größe eines Unternehmens abhängig.**

- Die **Benennung eines betrieblichen Datenschutzbeauftragten** ist laut DSGVO erforderlich, wenn
  - in der Regel mehr als 10 Personen im Unternehmen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder
  - „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“ oder
  - die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung besonderer Datenkategorien besteht (Gesundheitsdaten, Daten bzgl. Straftaten oder strafrechtlicher Verurteilungen, Daten zum Sexualleben und vergleichbar sensible Daten) oder
  - das Unternehmen laut DSGVO verpflichtet ist, eine Datenschutz-Folgenabschätzung durchzuführen oder
  - Daten geschäftsmäßig zum Zwecke der Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

- Im Wesentlichen ist es die **Aufgabe eines Datenschutzbeauftragten** laut DSGVO
  - Unternehmensangehörige über die Pflichten laut DSGVO aufzuklären und deren Einhaltung zu überwachen,
  - als Ansprechpartner für behördliche Anfragen sowie Anfragen von Betroffenen zur Verfügung zu stehen,
  - das Verarbeitungsverzeichnis zu führen,
  - Unternehmen, so weit für sie laut Art. 35 DSGVO vorgeschrieben, bei der Durchführung der Datenschutz-Folgenabschätzung zu unterstützen und
  - als unternehmensinterner Ansprechpartner in Fragen des Umgangs mit personenbezogenen Daten zudienen.

MIT WELCHEN VORRANGIGEN MASSNAHMEN SOLL DIE DSGVO UMGESETZT WERDEN?

Privacy by Design – Datenschutz durch Technikgestaltung
Bereits bei der Entwicklung von technischen und organisatorischen Systemen zur Datenverarbeitung werden Elemente nach den Anforderungen der DSGVO integriert.

Privacy by Default – Datenschutz durch datenschutzfreundliche Voreinstellungen
Dem Nutzer wird die Aufgabe der Auswahl von Einstellungen zum Schutz seiner Privatsphäre weitgehend abgenommen, indem ohne sein Zutun im „default", also im voreingestellten Modus, maximaler Privatsphäre-schutz ausgewählt ist.

Zertifizierung
Der Einsatz zertifizierter Systeme, zum Beispiel nach ISO 27001, bietet Unternehmen Sicherheit in der Einhaltung der Vorgaben der DSGVO.

Pseudonymisierung über TrustCenter
Daten stehen dem Unternehmen nur in einer Form zu Verfügung, die keine direkten Rückschlüsse auf die Person zulässt. Die Verknüpfung von Daten und Personen erfolgt über das TrustCenter.

Zudem werden Methoden der Pseudonymisierung wie Data Masking und Hashing eingesetzt.

Sollen Daten, zum Beispiel zu statistischen Zwecken, auch nach einem Löschauftrag, zum Beispiel durch den Betroffenen selber, erhalten bleiben, ist dies ausschließlich in vollständig anonymisierter Form erlaubt.

Datenminimierung / Datensparsamkeit / Datenvermeidung
Grundsätzlich sollen nur Daten erhoben werden, die konkret genutzt werden und insofern erforderlich sind. Bsp.: Für den Versand eines Newsletters ist kein Grund ersichtlich, warum eine Postadresse oder das Alter des Empfängers abgefragt wird. Für eine Geburtstagsliste sind grundsätzlich nur Tag und Geburtsmonat erforderlich, das Geburtsjahr nicht.

Beschränkung des Datenzugriffs
Im internen Gebrauch von personenbezogenen Daten sollen Systeme eingeführt werden, die verschiedenen Anwendern nur den Zugriff auf für sie nachweislich relevante Daten gestattet. Der Zugriff muss immer protokolliert werden.

Differential Privacy

Um die Zuordnung einzelner Datensätze zu konkreten Personen zu erschweren, muss bei der Datenbankabfrage eine Minimalgröße erreicht werden. Je mehr Datensätze abgefragt werden, desto schwerer ist es, durch einzelne Merkmale eine Person zu identifizieren.

Alternativ werden Datensätze automatisch geringfügig verändert und so ein „Rauschen“ hinzugefügt, das eine Rückverfolgung, bei möglichst erhaltener Genauigkeit der Daten, zusätzlich erschwert.

State of the art Verschlüsselung

Datenübertragung erfolgt ausschließlich verschlüsselt. Dabei wird der aktuelle Stand der Verschlüsselungstechnik genutzt.

Prüfpfade

Für jeden Datensatz muss zu jeder Zeit einfach belegbar sein, wie und wann die Daten erhoben wurden und in welcher Form der Betroffene hierzu sein Einverständnis erklärt hat.

Bitte beachten Sie, dass die hier aufgeführten Informationen natürlich nach bestem Wissen und Gewissen zusammengetragen und überarbeitet wurden, um Ihnen ein Maximum an Nutzwert zu bieten. Trotzdem stellen die hier aufgeführten Informationen keine Rechtsberatung dar. Für die Umsetzung der Datenschutz-Grundverordnung in Ihrem Unternehmen sollten Sie immer entsprechend qualifizierte Fachleute heranziehen, um über jeden, schlimmstenfalls kostspieligen, Zweifel in der Gesetzeskonformität erhaben zu sein.

QUELLEN

https://pr-journal.de/fragen-und-meinungen/autoren-beitraege-themen-der-zeit/20054-die-eu-dsgvo-als-chance-nutzen.html

https://www.e-recht24.de/datenschutzgrundverordnung.html

https://www.e-recht24.de/artikel/datenschutz/10744-datenschutzbeauftragter-dsgvo.html

https://www.wortkind.de/blog/neue-eu-datenschutzregeln-2018-tipps-kleine-unternehmen

http://www.ispd.de/MediaLibrary/Catalog/web/ispd/hersteller/ESET-Quick-Guide-zur-EU-Datenschutzgrundverordnung.pdf

https://www.mailjet.de/dsgvo/

https://www.lto.de/recht/hintergruende/h/eu-parlament-datenschutz-grundverordnung-dsgvo-reform-harmonisierung-bussgeld/

https://de.wikipedia.org/wiki/Datenschutz-Grundverordnung#Sanktionen

https://de.wikipedia.org/wiki/Personenbezogene_Daten

https://de.wikipedia.org/wiki/Bundesdatenschutzgesetz

unn | UNITED NEWS NETWORK GmbH
Lorenzstraße 29
D-76135 Karlsruhe

Telefon: +49 721 987793-30
Fax: +49 721 987793-11
E-Mail: service@lifepr.de
Web: www.lifepr.de

Handelsregister: Registergericht Mannheim (HRB 110836)
USt-IdNr.: DE 313899514
Geschäftsführer: Filip Jakubicek

life PR