BS FISI München

DATENSCHUTZ

EU-DSGVO

Informationsblatt

- Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union sowie Artikel 16 Absatz 1 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.siehe Verordnung Seite 1/(1)

- Ab dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO) der EU. Nach zweijähriger Übergangsfrist gelten einheitliche Regeln für alle 28 Mitgliedsländer und diese schaffen für 500 Millionen Menschen in der EU einen einheitlichen Datenschutzstandard.

- Anders als die Vorgängerregelung aus dem Jahr 1995 ist die DSGVO keine Richtlinie, sondern eine Verordnung. Das heißt: Sie tritt in allen Mitgliedsländern sofort in Kraft, muss nicht wie eine Richtlinie erst in nationales Recht umgesetzt werden.

- Gleichzeitig ist auch ein neues BDSG Bundesdatenschutzgesetz in Kraft getreten. Dieses Gesetz ist nachrangiges Recht und dient insbesondere der Regelung des Datenschutzes im öffentlichen Bereich, d.h. bei der Verarbeitung personenbezogener Daten durch Behörden und öffentliche Stellen.

- Wichtige Grundregeln, die in der DSGVO umgesetzt wurden:

1. Recht auf Vergessen, Datenportabilität und Zugang
2. Klare Einwilligung als Eckpfeiler
3. Informationsrechte und Transparenz
4. Strenge Regeln für Datentransfers in Drittstaaten
5. Zukunftstaugliche Definitionen
6. Harte Sanktionen von bis zu 4 Prozent des weltweiten Jahresumsatzes eines Unternehmens bei Verstößen
7. Datenschutzkonforme Technikgestaltung: Privacy by Design und by Default
8. Weniger Bürokratie
9. Einheitliche Rechtsdurchsetzung
10. Feste Ansprechpartner für Datenverarbeiter in ganz Europa

Quelle: https://www.janalbrecht.eu/2018/05/2012-12-12-alles-wichtige-zur-datenschutzreform/

Arbeitsauftrag

Bearbeiten Sie mit Hilfe der DSGVO folgende Aufgaben.

1. Wie lautet das Ziel und der Anwendungsbereich der DSVGO, welche in den Artikeln 1 und 2 genannt werden?

2. Welchen räumlichen Bereich umfasst die DSGVO im Artikel 3?

3. Erklären Sie folgende Begriffe, die in der DSGVO (Artikel 4) genannt werden und nennen Sie passende Beispiele:

   personenbezogene Daten:

   Verarbeitung:

   Profiling:

   Pseudonymisierung:

4. Nennen Sie die Unterschiede zwischen Verantwortlicher, Auftragsverarbeiter, und Empfänger.

5. Beschreiben Sie kurz folgende Grundsätze für die Verarbeitung personenbezogener Daten:

   Verarbeitung nach Treu und Glauben

   Zweckbindung

   Datenminimierung

   Richtigkeit

   Speicherbegrenzung

6. Welche personenbezogenen Daten dürfen nicht verarbeitet werden? Begründen Sie.

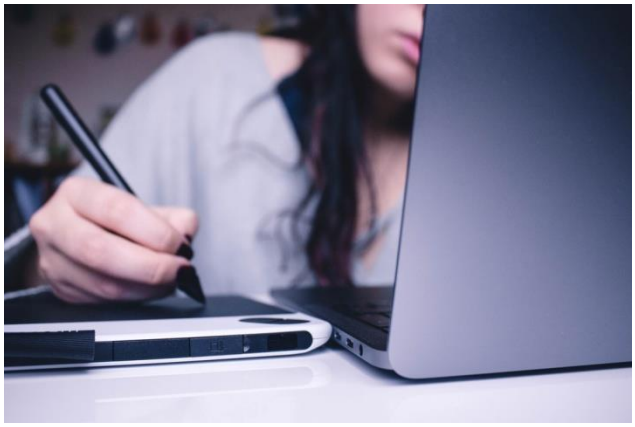
7. Im Artikel 32 der DSGVO und ergänzend im BDSG §64, wird die Sicherheit der Verarbeitung beschrieben.

   Nennen Sie technische und organisatorische Maßnahmen, die die Sicherheit gewährleisten können. Finden Sie jeweils praktische Beispiele zur Umsetzung dieser Maßnahmen.

Arbeitsauftrag

Markieren Sie wichtige praktische Punkte der folgenden Inhalte der DSGVO und nennen Sie die entsprechenden Artikel der DSGVO.

Einwilligung



Artikel DSGVO:

Ein wichtiger Eckpfeiler der Datenschutzgrundverordnung ist die Einwilligung. Hierdurch wird der Einzelne in die Lage versetzt, selbst zu entscheiden, wer welche Daten von ihm oder ihr erhalten, nutzen und speichern dürfen soll.
Neu sind die hohen Anforderungen, die an diese Einwilligung gestellt werden. Bisher war es so, dass Unternehmen gerne eine stillschweigende Einwilligung der Nutzer fingiert haben: Facebook hat beispielsweise das simple Anmelden auf der Plattform als Einwilligung in zwischenzeitlich geänderte Nutzungs- und Datenschutzerklärungen interpretiert. Auch wurden Einwilligungen durch voreingestellte Haken in Kästchen erhascht, welche die Nutzer bisher erst aufmerksam wieder entfernen mussten. Solche Praktiken sind fortan nicht mehr möglich. Die Einwilligung der betroffenen Person muss – als Ausdruck ihres Selbstbestimmungsrechts – informiert, freiwillig und eindeutig durch eine Zustimmungshandlung erklärt worden sein:

1. Informiertheit
Um eine Einwilligung zu erteilen, muss die betroffene Person wissen, worein sie überhaupt einwilligen soll. Dafür muss in klarer und verständlicher Sprache erklärt werden, wer zu welchen Zwecken die Daten verarbeitet. Darüber hinaus müssen umfangreiche Informationen etwa über die Speicherdauer der Daten und die Rechte der betroffenen Person bereitgestellt werden. Vorformulierte Einwilligungserklärungen dürfen zudem keine missbräuchlichen Klauseln enthalten.

2. Eindeutige Zustimmungshandlung
Jede Einwilligung bedarf zudem einer klaren zustimmenden Handlung. Eine stillschweigende Einwilligung eines Nutzers, die er oder sie im Zweifel also gar nicht mitbekommen hat, wie etwa im Facebook-Beispiel, ist somit nicht mehr möglich. Um eine wirksame Einwilligung in eine Datenverarbeitung zu erteilen muss die betroffene Person fortan aktiv beteiligt werden, etwa durch das eigenständige Setzen eines Hakens in einem Kästchen (sogenanntes „Opt-in“). Auch die heutige Praxis, Cookie-Banner einzublenden und bereits ohne den Klick auf „ok“ personenbezogene Daten der Website-NutzerInnen zu verarbeiten, genügt den Anforderungen an eine wirksame Zustimmungshandlung nicht.

3. Freiwilligkeit
Die betroffene Person muss außerdem eine echte Wahl haben, ob sie einwilligen möchte, oder nicht. Aufgrund des sogenannten „Kopplungsverbots“ darf daher auch das Erbringen einer Leistung nicht von einer Einwilligung in Datenverarbeitungen abhängig gemacht wird, die für die Abwicklung des Geschäfts überhaupt nicht benötigt werden. Dies soll verhindern, dass Betroffene oft Angebote im Internet nur dann nutzen können, wenn sie Daten von sich Preis geben, die für den Dienst überhaupt nicht erforderlich sind. Die verbreitete Praxis, bei der Installation von beispielsweise einer Taschenlampen-App eine Einwilligung die Übermittlung der Standortdaten des Smartphone-Nutzers zu erzwingen, ist deshalb fortan nicht mehr möglich.

4. Form
Die Datenschutzgrundverordnung sieht keine spezielle Form der Einwilligungserklärung vor, und stellt klar, dass die Einwilligung auch elektronisch und beispielsweise durch Anklicken eines Kästchens beim Besuch einer Internetseite oder durch die Auswahl technischer Einstellungen im Browser möglich ist.

Recht auf Vergessen, Datenportabilität und Zugang

Artikel DSGVO:

Mit der Datenschutzgrundverordnung wird – als Weiterentwicklung des bereits existierenden Rechts auf Löschung – ein „Recht auf Vergessenwerden“ gesetzlich verankert. Wer möchte, dass seine persönlichen Daten gelöscht werden, kann sich dafür direkt an Google, Facebook und Co. wenden. Ist bspw. die Speicherung der Daten nicht mehr notwendig, oder widerruft man eine vormals erteilte Einwilligung zur Speicherung der Daten, sind die Unternehmen grundsätzlich verpflichtet, dem Löschungsbegehren nachzukommen. Dann darf sich das Unternehmen nur noch in engen Ausnahmefällen der Löschung verwehren – etwa im Fall von z.B. Prominenten, bei denen das Interesse der Öffentlichkeit an bestimmten Informationen das Interesse der/des Prominenten an der Löschung überwiegen kann.
Mit dem „Recht auf Vergessenwerden“ wird künftig sichergestellt, dass Unternehmen, welche die Daten öffentlich gemacht hatten, das Löschungsverlangen sogar an Dritte weiterleiten müssen, wenn diese auf die Veröffentlichung verweisen. Zusätzlich dazu muss das Unternehmen auch allen sonstigen Dritten, welchen es die Daten weitergeleitet hatte, das Löschungsbegehren mitteilen. So werden nach Möglichkeit sämtliche Kopien der Daten gelöscht werden und die betroffene Person tatsächlich „vergessen“ werden.
Auch ein Widerspruch gegen die Verarbeitung der eigenen Daten ist möglich – und dies künftig auch automatisiert, z.B. durch Browser-Einstellungen wie „Do not Track“. Bei Aktivieren dieser mittlerweile in jedem Browser verfügbaren Einstellung sind die Webseitenbetreiber also dazu gezwungen, dies als rechtswirksamen Widerspruch zu akzeptieren und somit daran gehindert, Nutzungsdaten zu speichern und Nutzungsprofile zu erstellen.

Neu ist außerdem das Recht auf den Umzug eigener Daten, etwa beim Anbieterwechsel („Datenportabilität“). Dadurch ist es nun leichter möglich, von einem sozialen Netzwerk, E-Mail-Dienst oder Fitnessarmband-Hersteller zu einem anderen zu wechseln. Um dies zu ermöglichen, muss der Anbieter die Daten in einem gängigen interoperablen Format zur Verfügung stellen.
Darüber hinaus sollen Anbieter kostenfrei und schnell die Nutzerdaten auf Anfrage auf elektronischem Weg aushändigen, sodass sich jeder ein Bild von den über sich gespeicherten Daten machen kann.

Informationsrechte und Transparenz

Artikel DSGVO:

Die Welt der Datenverarbeitung ist oft undurchsichtig und es ist schwer nachzuvollziehen, wer welche Daten von einem verarbeitet, zu welchen Zwecken dies geschieht, und wohin diese Daten vielleicht noch weitergegeben werden. Um der betroffenen Person wieder mehr Kontrolle über ihre Daten zu geben, sind diese Informationen jedoch unerlässlich. Insbesondere zu Zeiten des Internets der Dinge, in der sogar mein Kühlschrank oder Staubsauger personenbezogene Daten von mir verarbeitet, muss ich wissen, dass es überhaupt zu einer Verarbeitung kommt und an wen ich mich wenden kann, wenn ich von meinen Rechten gegenüber Datenverarbeitern Gebrauch machen will. Transparenz und Information sind somit Grundvoraussetzung des Selbstbestimmungsrechts des Einzelnen.
Aus diesem Grund beinhaltet die neue Datenschutzgrundverordnung ausdrücklich einen Transparenzgrundsatz. Er umfasst insbesondere folgende Information:

- Informationen über diejenigen, die die Daten verarbeiten
- zu welchen Zwecken die Daten verarbeitet werden
- auf welcher Rechtsgrundlage die Daten verarbeitet werden
- wenn die Verarbeitung auf der Einwilligung der betroffenen Person beruht die Möglichkeit zum jederzeitigen Widerruf der Einwilligung
- die der Person zustehenden Betroffenenrechte
- ob die Daten in ein Drittland übermittelt werden sollen
- die Speicherdauer der Daten
- wenn die Daten nicht bei der betroffenen Person erhoben werden, aus welcher Quelle die Daten stammen und die Kategorien der personenbezogenen Daten, die verarbeitet werden

Die Informationen müssen der betroffenen Person in klarer und verständlicher Sprache zur Verfügung gestellt werden. Um den Nutzern das Verständnis zu erleichtern und ihnen zu ersparen, sich durch lange Datenschutzerklärungen zu wälzen (was in der Praxis ohnehin kaum geschieht), kann dies auch durch standardisierte Bildsymbole (Icons) geschehen, welche die Kommission veröffentlichen würde und den Unternehmen zur Nutzung zur Verfügung gestellt würden.
Wenn eine betroffene Person eines ihrer Betroffenenrechte geltend macht, muss das Unternehmen die Person zudem anschließend informieren, welche Schritte er unternommen hat, um dem Recht nachzukommen. All diese Informationen müssen der betroffenen Person kostenfrei zur Verfügung

gestellt werden.
Verstöße gegen die Informationspflichten werden mit empfindlichen Sanktionen geahndet.

Strenge Regeln für Datentransfers in Drittstaaten

Artikel DSGVO:

Die Datenschutzgrundverordnung stellt strenge Regeln für die Übermittlung personenbezogener Daten in sogenannte Drittländer – also solche, die nicht zur EU gehören – auf. Dies ist besonders wichtig, da das Grundrecht auf Privatsphäre und Datenschutz eine Besonderheit hat: Anders als beispielsweise unsere ebenfalls grundrechtlich geschützte körperliche Unversehrtheit, die untrennbar mit uns und damit unserem Aufenthaltsort verbunden ist, können unsere Daten auch getrennt von uns sein, weitergegeben werden und sich an vollkommen anderen Orten befinden, als wir es gerade sind. Daher muss unser Recht auf Privatsphäre und Datenschutz mit ihnen – auch über die Grenzen der EU hinweg – mitreisen können. So wird sichergestellt, dass auch wenn unsere Daten im Ausland verarbeitet oder gespeichert werden, wir die gleichen Rechte, wie etwa auf Auskunft oder Löschung, haben.
Dies ist in der praktischen Anwendung der DSGVO besonders relevant, da viele der Server, auf denen unsere Daten beispielsweise bei der Nutzung eines Cloud-Services wie Dropbox gespeichert werden, nicht in der EU stehen. Zudem haben die größten IT-Dienstleister wie Microsoft, Facebook oder Google ihren Hauptsitz sowie viele ihrer Rechenzentren in den USA. Wenn sie EU-Bürger zu ihren Kunden zählen, müssen sie jedoch die strengen Übermittlungsregeln der Verordnung beachten:
Nach der sogenannten 2-Stufen-Prüfung muss auf erster Stufe eine Rechtsgrundlage bestehen, aufgrund derer die Daten überhaupt verarbeitet werden dürfen. Diese erste Stufe gilt auch für Datenverarbeitungen in der EU – die Verarbeitung ist grundsätzlich verboten, außer es besteht eine gesetzlich normierte Erlaubnis. Auf der zweiten Stufe muss bei Datentransfers ins außereuropäische Ausland darüber hinaus beim Datenempfänger ein angemessenes Datenschutzniveau sichergestellt sein.
Dies kann etwa durch allgemeingültige Angemessenheitsbeschlüsse der Europäischen Kommission geschehen, die die Datenschutzregimes anderer Staaten überprüft und für diese verbindlich feststellen kann, dass der dortige Datenschutz im wesentlichem dem unserem entspricht. Für Kanada und Argentinien zum Beispiel besteht ein solcher Angemessenheitsbeschluss. Drittstaaten haben aus wirtschaftlichen Gründen oft besonderes Interesse daran, einen solchen Angemessenheitsbeschluss zu erlangen, sodass sie versuchen, ihre Datenschutzregimes an unseres anzupassen. So arbeiten beispielsweise gerade Japan und Jamaika an der Überarbeitung ihrer Datenschutzgesetze. Die Datenschutzgrundverordnung wird somit ein Stück weit zum Weltstandard.

Weitere Möglichkeiten der Datenübermittlung in unsicherere Länder sind unternehmensspezifische Zertifizierungen durch die Datenschutzbehörden oder vertragliche Vereinbarungen mit dem Datenempfänger.
In jedem Fall müssen die Betroffenenrechte und die Schutzstandards im Empfängerland „der Sache nach gleichwertig“ sein, so der Europäische Gerichtshof in seinem Urteil, das die „Safe Harbor“-Vereinbarung mit den USA aufhob. Die Nachfolgevereinbarung „Privacy Shield“, die derzeit Datenübermittlungen in die USA erlaubt, wird absehbar wieder vor dem Gerichtshof landen.

Quelle: https://www.janalbrecht.eu/2018/05/2012-12-12-alles-wichtige-zur-datenschutzreform/