Die EU-Datenschutz-Grundverordnung und die Anforderungen an Big Data

Fabian Richter

Seminararbeit im Interdisziplinären Lehrangebot
des Instituts für Informatik

Leitung: Prof. Hans-Gert Gräbe, Ken Pierre Kleemann

`http://bis.informatik.uni-leipzig.de/de/Lehre/Graebe/Inter`

Leipzig, 30.09.2018

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Einleitung

1.1 Problemstellung

Dieser Arbeit vorausgegangen ist eine Präsentation zum Thema „EU-Datenschutz-Grundverordnung (DSGVO) und die damit verbundene Privatsphäre im Internet“. Bei der Recherche und Erstellung dieser Präsentation, sind die neuen Anforderungen an Big Data und ein gewisses Maß an Konfliktpotenzial dieser Thematik deutlich geworden und somit in den Fokus dieser Seminararbeit gerückt.
Seit einigen Jahren hat der Begriff Big Data an Stellenwert und Aufmerksamkeit gewonnen. Schon im Jahr 2013 wurde dieser von der Gesellschaft für deutsche Sprache auf Platz 5 der Wahl für das Wort des Jahres gewählt (vgl. GfdS, Wort, 2013, o.S.). Auch im vergangenen Jahr sorgte der Begriff für Aufsehen, da laut einem Artikel der Süddeutschen Zeitung, Donald Trump die US-Wahlen von 2016 mit Hilfe von Big Data Strategien für sich entschieden haben soll. Es wird berichtet, dass die Firma Cambridge Analytica große Daten verwendet hat, um jedem potentiellen Wähler eine Wahlkampagne zu zeigen, die seiner Persönlichkeit angepasst ist (vgl. Grassegger, 2017, o.S). Dieser Vorfall macht deutlich, dass es fast unmöglich ist, sich dem Thema Big Data zu entziehen. Ob bei der Arbeit oder im privaten Bereich, bewusst oder unbewusst, ist jeder von uns ein Nutzer und ein Generator von Big Data. Während in Deutschland die Angst vor Überwachung und den Risiken sehr groß sind, wird Big Data von den Bürgern der USA als weniger negativ empfunden. Um die personenbezogenen Daten von EU-Bürgern einschließlich der Verarbeitung von Big Data zu schützen, haben das Europäische Parlament und der Rat der Europäischen Union 2016 die neue EU-Datenschutz-Grundverordnung veröffentlicht, die im Mai 2018 in Kraft getreten ist (vgl. Nitsch, K., Informatikrecht, 2018, S. 405 f). Die Europäische Kommission schätzt, dass der Wert der personenbezogenen Daten europäischer Bürger bis 2020 auf 1 Billion Euro ansteigen wird, weshalb es dringend erforderlich ist, diese durch ein neues Regelwerk zu schützen (vgl. Europäische Kommission, Datenschutzreform, 2015, o.S).

1.2 Ziele der Arbeit

Diese Seminararbeit zielt darauf ab, ein Grundverständnis für die neue EU-Datenschutz-Grundverordnung und Big Data zu vermitteln. Darüber hinaus sollte klargestellt werden,

welche Anforderungen für die Nutzung von Big Data erfüllt sein müssen, um die Anforderungen der EU-Datenschutzgverordnung zu erfüllen. Nach den einleitenden Worten über den Zweck und den Verlauf der Arbeit, wird im zweiten Kapitel eine Definition der Begrifflichkeiten von der DSGVO und Big Data gegeben, um für den Leser ein grundlegendes Verständnis für das Thema zu schaffen. Im dritten Kapitel wird eine Analyse der Anforderungen an Big Data unter Berücksichtigung der EU-Datenschutz-Grundverordnung durchgeführt. Zunächst werden die Anforderungen an den Datenschutz durch Design und Datenschutz standardmäßig besprochen, worunter Datenschutz durch technische Gestaltung und datenschutztechnische Voreinstellungen verstanden werden. Danach folgen die Anforderungen für die Verarbeitung personenbezogener Daten und schließlich werden die Themen Auskunftspflicht und Informationspflicht behandelt. Die Arbeit endet mit einer Zusammenfassung, die die Ergebnisse zusammenfasst und einen Ausblick auf weitere Themen gibt.

2. Begriffliche Abgrenzung

2.1 Definition der neuen EU-Datenschutz-Grundverordnung (DSGVO)

Im Folgenden werden die beiden Begriffe EU-Datenschutz-Grundverordnung und Big Data ausführlicher beschrieben, da diese einen Hauptbestandteil dieser Seminararbeit ausmachen. „Die DSGVO kümmert sich um den Schutz der Daten von natürlichen Personen. Ziel ist das jede Person bestimmen kann, wer, wann und welche persönlichen Informationen über sie sammelt, speichert und verarbeitet. Ziel dieser Verordnung ist die Harmonisierung von Datenschutzbestimmungen der Europäischen Union und die stärkere Kontrolle von natürlichen Personen über eigene Daten.“ (Präsentation „EU-Datenschutz Grundverordnung und die damit verbundene Privatsphäre im Internet“, 2018). Die DSGVO ist damit deutlich von der Informationssicherheit abzugrenzen, die sich mit dem Schutz aller Arten von Informationen vor Verlust, Diebstahl, Sabotage oder Missbrauch befasst. Die erste Datenschutzrichtlinie entstand 1995 und musste aufgrund der technischen Entwicklung in den letzten 20 Jahren und der damit verbundenen Datenschutzanforderungen geändert werden. Daher haben das Europäische Parlament und der Rat der Europäischen Union 2016 die neue EU-Datenschutz-Grundverordnung veröffentlicht, die am 25. Mai 2018 für alle EU-Mitgliedstaaten in Kraft getreten ist und die alte Datenschutzrichtlinie abgelöst hat (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, S.405). Die

Gesetzesverordnung besteht aus elf Kapiteln, die insgesamt 99 Artikel enthalten. Die ersten 50 Artikel befassen sich mit Fragen des Datenschutzes, die übrigen 49 mit organisatorischen und formalen Fragen (vgl. Roßnagel, 2016, S. 156). Den elf Kapiteln gehen 173 Erwägungsgründe voraus, die zur Verabschiedung dieser Verordnung führten und weitere Erläuterungen enthalten. Insgesamt verfolgen das Europäische Parlament und der Rat der Europäischen Union daher zwei Ziele. Einerseits sollte die derzeitige europäische Norm harmonisiert und an den technologischen Fortschritt angepasst werden. Andererseits sollten die personenbezogenen Daten natürlicher Personen während der Weiterverarbeitung geschützt und die freie Übermittlung dieser geschützten Daten sichergestellt werden. Als personenbezogene Daten bezeichnet die EU-Datenschutzverordnung Informationen, die einer bestimmten oder bestimmbaren Personen zugewiesen werden können. Zu diesen Informationen zählen unter anderem Standortdaten, Namen, Online-Identifizierungen oder kulturelle oder soziale Identitäten (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 4 Abs. 1 DSGVO). Unabhängig von dem Land, in dem die Verarbeitung personenbezogener Daten stattfindet, gilt die Verordnung, wenn die Verarbeitung aufgrund eines Verantwortlichen innerhalb der Europäischen Union erfolgt. Das bedeutet, wenn die personenbezogenen Daten von Bürgern der Europäischen Union zugeordnet werden können, aber von einer Person außerhalb der Union verarbeitet werden, die Verordnung trotzdem in Kraft tritt. Verglichen mit der Richtlinie aus dem Jahr 1995 konnten die EU-Mitgliedstaaten die Rechtsgrundsätze in ihrem nationalen Recht unterschiedlich umsetzen - Die EU-Datenschutz-Grundverordnung ist für alle Staaten einheitlich und verbindlich. Die Europäische Kommission geht davon aus, dass Unternehmen durch Einführung dieser einheitlichen Rechtsgrundlage jährlich bis zu 2,3 Mrd. € einsparen können. Diese Kosteneinsparungen ergeben sich aus der Tatsache, dass Unternehmen in den jeweiligen Ländern bei der grenzüberschreitenden Datenverarbeitung einheitlich aufgestellt werden können und nicht an die jeweiligen nationalen Gesetze angepasst werden müssen (vgl. Europäische Kommission, Datenschutzreform, 2015, o.S). Trotz des Ziels der Harmonisierung bietet sie dennoch die Möglichkeit für die Mitgliedstaaten, bestimmte spezifische Regeln festzulegen. Im Falle eines Verstoßes gegen diese Verordnung kann die verantwortliche Person jedoch mit einer Geldstrafe von bis zu 20 Mio. EUR oder bis zu 4% des im Vorjahr erzielten weltweiten Jahresumsatzes rechnen. Nach Artikel 30 sind die Verantwortlichen daher auch verpflichtet alle ihre Verarbeitungstätigkeiten zu dokumentieren. Diese Dokumentation muss schriftlich oder in elektronischer Form der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden (vgl.

Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 5 Abs. 2 DSGVO & Art. 30 Abs. 1-4 DSGVO; Duda, D., Dokumentationspflichten, 2017, S. 9).
Ausdrücklich ist der Begriff Big Data in der EU-Datenschutz-Grundverordnung nicht direkt aufgeführt oder beschrieben. Jedoch verbergen sich hinter dem Begriff *Profiling* Big Data Analysen. Dieser Ausdruck bezieht sich auf die gesamte automatisierte Verarbeitung personenbezogener Daten, die unter anderem zur Analyse oder Vorhersage der Arbeitsleistung, der wirtschaftlichen Situation, der persönlichen Präferenzen und des Verhaltens von Einzelpersonen dient (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 4 Abs. 4 DSGVO; S. 585). Detailliertere Regeln für die Erstellung von Profilen finden sich in Artikel 22 der Verordnung. Sie besagt, dass Entscheidungen, die eine Rechtswirkung haben oder andere in ähnlicher Weise betreffen, wie eine automatische Ablehnung eines Online-Kreditantrags oder ein Einstellungsverfahren, nicht ausschließlich auf der Grundlage einer automatisierten Verarbeitung erfolgen können. In solchen Fällen muss die verantwortliche Person jedoch Maßnahmen ergreifen, um die Rechte und Freiheiten der betreffenden Person zu schützen, einschließlich zumindest des Eingreifens einer Person (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 22 Abs. 3 DSGVO; S. 168). In den folgenden Kapiteln werden die Anforderungen an Datenschutz durch Design und datenschutzfreundliche Voreinstellung, personenbezogene Daten, Informationspflicht und die Verpflichtung zur Bereitstellung von Informationen in der EU-Datenschutzverordnung erörtert, die die Richtlinien für den Umgang mit Big Data bilden.

2.2 Definition Big Data

Alle Nutzer von technischen Produkten, Dienstleistungen und Kommunikationsmedien erstellen Daten, die von Unternehmen weiterverarbeitet werden, um mehr Produkte, Dienstleistungen oder Innovationen zu schaffen. Durch diesen Vorgang werden zusätzliche neue Daten von Benutzern erstellt. Diese großen Datenmengen sind die Basis für Big Data (vgl. Nieendick, M., Jansen, J., Kalinowski, T., Big Data, 2018, S. 245 f; Bachmann, R., Kemper, G., Gerzer, T., Big Data, 2014, S. 23; Freiknecht, J., Big Data, 2014, S. 10). Bitkom, der 1999 den digitalen Verband gründete, betont bei der Definition von Big Data, dass diese Daten in einem unbekannten Ausmaß wachsen können und sich schnell ändern können. Darüber hinaus sind diese Datensätze in verschiedenen Strukturen verfügbar. Das Ziel

besteht darin, aus diesen Informationen wirtschaftlich aussagekräftige Erkenntnisse zu gewinnen (vgl. Bitkom, Bitkom, o.J., o. S; Bitkom, Praxiseinsatz, 2012, S. 19). In der Literatur wird der Rahmen von Big Data häufig durch die drei Eigenschaften Volumen, Geschwindigkeit und Vielfalt beschrieben. Diese werden durch die Eigenschaft Veracity ergänzt. Das Volumen steht für die große und stetig wachsende Datenmenge, die für die Big-Data-Analyse zur Verfügung steht. Durch diese Eigenschaft ist es möglich, datengetriebene Hypothesen über viele Lebensbereiche hinweg zu erstellen. Die zweite Eigenschaft ist die Geschwindigkeit. Sie beschreibt die Schnelligkeit, mit der die Daten verarbeitet und ausgewertet werden können. Da jedoch weitere Daten genauso schnell hinzugefügt werden, sind die Ergebnisse innerhalb eines kurzen Zeitraums wieder veraltet. Die dritte Eigenschaft beschreibt die Vielfalt der gesammelten Daten, da die Datenmengen bei der Gewinnung nicht strukturiert sind und eine Vielzahl von Inhalten aus verschiedenen Quellen und in verschiedensten Formaten, wie Text-, Video- und Audiodateien, vorliegen. Diese müssen zunächst strukturiert werden, um eine Datenanalyse durchführen zu können. Hinter der vierten Eigenschaft verbirgt sich der Begriff Richtigkeit (engl. Veracity). Er charakterisiert die Genauigkeit, Vollständigkeit und Zuverlässigkeit des Datensatzes, da die Big-Data Mengen auch Daten umfassen, die unterschiedliche Qualitäten aufweisen. Mit speziellen Algorithmen können diese Datenqualitäten ausgewertet werden (vgl. Freiknecht, J., Big Data, 2014, S. 13 f; Meier, A., Kaufmann, M., Datenbanken, 2016, S.13). Die schnelle Verfügbarkeit und Auswertung der Daten ermöglicht es, die Fakten unterschiedlich zu bewerten und neue Sachverhalte entstehen zu lassen. Durch die Anwendung neuer Technologien, können nun datengetriebene Hypothesen entwickelt werden (vgl. Wrobel, S., Voss, H., Köhler, J., Beyer, U., Auer, S., Big Data, 2015 S. 371). Insbesondere in Fällen, in denen keine absolute Sicherheit vorliegt, aber eine hohe Wahrscheinlichkeit ausreicht, bieten Big-Data-Analysen und ihre Vorhersagen eine hilfreiche Grundlage für die Entscheidung. Somit kann die Big-Data-Analyse in vielen Bereichen eingesetzt werden und dazu beitragen, die Effizienz von Unternehmen zu steigern, Täter im Sicherheitsbereich zu analysieren, Marketing personenbezogen zu platzieren und auch Einfluss auf politische Wahlkampagnen zu nehmen (vgl. Roßnagel, A., Geminn, C., Jandt, S., Richter, P., Datenschutz, 2016, S. 24). Zusammengefasst beschreibt Big Data die Nutzung und Analyse großer Datenmengen aus mehreren Quellen mit einer hohen Verarbeitungsgeschwindigkeit für die Erzeugung von wirtschaftlichen Vorteilen.

3. Die Nutzung von Big Data mit der EU-Datenschutz-Grundverordnung

3.1 Technikgestaltung und datenschutzfreundliche Voreinstellungen

Artikel 25 der EU-Datenschutz-Grundverordnung listet die Aspekte des Datenschutzes durch Technologiedesign und datenschutzfreundliche Voreinstellungen auf, die in diesem Kapitel ausführlicher beschrieben werden. In einem *Factsheet* aus dem Jahr 2015 weist die Europäische Kommission diesen beiden Aspekten eine zentrale Rolle bei der weiteren Nutzung von Big Data zu.

Datenschutz durch Technologiedesign wird im Fachjargon auch als *Privacy by Design* bezeichnet. Folglich sollte bei der Entwicklung neuer Datenverarbeitungstechniken bereits darauf geachtet werden, dass Datenschutzmaßnahmen wie Pseudonymisierung und Datenverarbeitungstechniken möglichst geringgehalten werden (vgl. Europäische Kommission, Datenschutzreform, 2015). Die EU-Datenschutzgrundverordnung greift diesen Punkt ebenfalls auf, um sicherzustellen, dass personenbezogene Daten zum Zeitpunkt der Bestimmung und der Verarbeitung durch technische und organisatorische Maßnahmen datenschutzrechtlich geschützt sind. Die Verordnung führt ausdrücklich eine Pseudonymisierung ein, um der Minimierung von Daten gerecht zu werden, und enthält Maßnahmen die dem Schutz personenbezogener Daten dienen (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 25 Abs. 1 DSGVO). Pseudonymisierung wird in der Verordnung wie folgt erläutert. Der Begriff Pseudonymisierung bedeutet, dass personenbezogene Daten nicht mehr einer bestimmten Person zugeordnet werden können, ohne dass zusätzliche Informationen hinzugezogen werden. Diese zusätzlichen Daten müssen getrennt gespeichert werden, so dass keine direkte Verbindung besteht, die Rückschlüsse zulassen würde. Es muss auch technische und organisatorische Maßnahmen geben, die eine direkte Zuordnung verhindern (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 4 Abs. 5 DSGVO).

Die datenschutzfreundlichen Standardeinstellungen werden als *Privacy by Default* beschrieben. Darunter ist die Anforderung zu verstehen, dass direkt bei der ersten Nutzung eines IT-Systems benutzerfreundliche Datenschutzbestimmungen erfüllt sind und nicht nur, wenn der Nutzer diese Einstellung selbst vornimmt oder ändert. Dies kann oft schon während der Entwicklung sichergestellt werden (vgl. Kipker, D., Datenschutz, 2015, S. 410). Des Weiteren sind diese Anforderungen auch in Artikel 25 der DSGVO wiederzufinden. Vorgegebene technische oder organisatorische Maßnahmen sollen sicherstellen, dass von

Anfang an nur die notwendigen personenbezogenen Daten verarbeitet werden (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 25 Abs 2 DSGVO). Nur wenn der Nutzer selbst seine Datenschutzeinstellungen ändert, sollte der Zugriff auf andere Daten gewährt werden (vgl. Cavoukin, A., Prinzipien, 2009, S. 2; Hagendorff, T., Informationskontrolle, 2017, S. 157).

Die Europäische Kommission verfolgt außerdem das Ziel, die weitere Nutzung der Big-Data-Analyse durch die Verordnung zu unterstützen. Im Factsheet heißt es, dass die Verordnung folgende Maßnahmen fördert, damit die Daten dann für weitere Verarbeitung und Analysen genutzt werden können:

-Anonymisierung (Löschung unnötiger personenbezogener Daten)

-Pseudonymisierung (Ersetzung personenbezogener Daten durch Zeichenkombinationen)

-Verschlüsselung (Verschlüsselung von Nachrichten, so dass sie nur von autorisierten Personen gelesen werden können)

(vgl. Europäische Kommission, Datenschutzreform, 2015)

Eine gesonderte Definition, wann Daten als anonyme Daten zu klassifizieren sind, ist in der Verordnung nicht vorgesehen, kann jedoch aus der Beschreibung von personenbezogenen Daten abgeleitet werden. Dies erfordert die Beachtung der Mittel, die für die Identifizierung verwendet werden können. Um festzustellen, ob diese Mittel verwendet werden, dienen die Kosten und die Zeit für die Identifizierung und die zur Verfügung stehende Technologie und die zukünftig absehbaren technologischen Entwicklungen. Schlussendlich ist daher nicht eine unwiederbringliche Anonymität erforderlich, sondern ein Zustand zum Zeitpunkt der Erhebung, bei der eine erneute Identifizierung nicht wahrscheinlich erscheint (vgl. Schwartmann, R., Weiß, S., Pseudonymisierung, 2017, S. 13). Darüber hinaus ist auch nicht geklärt, ob die Daten anonym sind, wenn eine verantwortliche Person diese pseudonymisiert weitergibt und die Informationen nicht zur Wiederherstellung übermittelt. Die Informationen in Kapitel 2.2 über die Merkmale von Big Data, stellen eine große Herausforderung für die Anonymisierung personenbezogener Daten dar, da die Verknüpfung zusätzlicher Daten das Risiko einer erneuten Identifizierung von Personen erhöht. Alle vorherigen Konzepte zur Anonymitätsberechnung basieren auf einer statischen Datenmenge und bewerten das Ergebnis der Anonymisierung als dauerhaft konstant, allerdings abhängig vom technischen Fortschritt und der wachsenden Datenmenge und deren Verknüpfungen. In der DSGVO fehlen leider jegliche Angaben zur Qualität der Pseudonymisierung. Daher bietet sie den Unternehmen somit die Möglichkeit, eine Variante der Pseudonymisierung zu wählen, welche für die Identifizierung von privaten Personen am

einfachsten rückgängig gemacht werden kann (vgl. Marnau, N., Pseudonymisierung, 2016, S. 429-431).

3.2 Verarbeitung von personenbezogenen Daten

Unter der Verarbeitung personenbezogener Daten versteht die EU - Datenschutzgrundverordnung alle manuellen oder automatisierten Verfahren, die bei der Erhebung, Verarbeitung, Übermittlung oder Vernichtung personenbezogener Daten eine Rolle spielen. Informationen zu den Bedingungen für die Verarbeitung dieser Daten enthält die Verordnung Artikel fünf, in dem die folgenden sechs Prinzipien aufgeführt werden.

1. Die Daten dürfen nur in einer nachvollziehbaren Art und Weise verarbeitet werden (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 5 Abs. 1 DSGVO).
2. Wird der Grundsatz Zweckbindung aufgeführt, der beschreibt, dass die Daten nur für einen festen, rechtmäßigen Zweck erhoben und für keinen anderen Zweck weiterverarbeitet werden dürfen. Wenn die Gründe der Erhebung vor der Verarbeitung klar definiert worden sind, können die Daten auch für mehrere Zwecke verarbeitet werden.
3. Das dritte Prinzip ist die Datenminimierung. Die Datenmengen sollten auf ein Minimum beschränkt werden, welches für die eigentliche Verarbeitung auch wirklich notwendig ist.
4. Die Daten sollten korrekt und aktuell sein und somit alle falschen Daten sofort gelöscht werden.
5. Die Informationen dürfen nur so lange gespeichert werden, wie es für den Zweck, für den sie verarbeitet wurden, notwendig ist.
6. Die Verarbeitung personenbezogener Daten muss durch geeignete technische und organisatorische Maßnahmen sichergestellt werden. Verantwortlich für die Einhaltung der sechs Punkte ist der Datenschutzverantwortliche. Letzterer muss auch in der Lage sein, die Einhaltung nachzuweisen (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 5 Abs. 1. DSGVO). Darüber hinaus enthält Artikel 6 die Gründe, aus denen mindestens ein Grund für die Rechtmäßigkeit der Verarbeitung der Daten gegeben sein muss. Dazu gehört unter anderem, dass die Zustimmung zur Verarbeitung für einen oder mehrere Zwecke der betroffenen Person gilt, dass die Verarbeitung rechtsverbindlich ist oder dass sie dazu dient, die lebenswichtigen Interessen einer natürlichen Person zu schützen.

Weitere Voraussetzungen für eine rechtmäßige Verarbeitung müssen bei der Verarbeitung personenbezogener Daten eines Kindes erfüllt sein. Zum Beispiel muss ein Erziehungsberechtigter der Verarbeitung zustimmen, wenn das Kind unter 16 Jahre alt ist. In diesem Fall erlaubt die Verordnung den Mitgliedstaaten, die Grenze auf Vollendung des 13. Lebensjahres zu reduzieren. Des Weiteren ist auch die Verarbeitung von Daten ohne Zustimmung oder für andere Zwecke als zum Zeitpunkt der ursprünglichen Datenerhebung unter bestimmten Umständen möglich. Unter anderem werden die möglichen Konsequenzen für die betroffenen Personen erwähnt und Garantien müssen verfügbar sein, um die Daten zu schützen. Geeignete Sicherheitsmaßnahmen umfassen dabei Verschlüsselung und Pseudonymisierung (vgl. Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 8 Abs. 1 und Art. 6 Abs. 4 DSGVO). Diese beiden Garantien ermöglichen die weitere Nutzung der Big-Data-Analyse bei einer späteren Änderung des Zwecks (vgl. Marnau, N., Pseudonymisierung, 2016, S. 432). Dementsprechend wird die Wahl des Datenverarbeitungsunternehmens für die Verantwortlichen in Zukunft gleich wichtig sein. Laut Kapitel 2.2. muss sichergestellt werden, dass der Bearbeiter alle gesetzlichen Anforderungen erfüllt, um das angesprochene Bußgeld zu vermeiden. Die Verarbeitung darf auch nur aufgrund eines Vertrages erfolgen, der unter anderem den Zweck und die Dauer der Datenverarbeitung, eine Verschwiegenheitspflicht und die Löschung der Daten nach Beendigung der Datenverarbeitung festlegt.

3.3 Auskunftsrecht und Informationspflicht

In Artikel 13 der EU-Datenschutz-Grundverordnung ist die Verpflichtung zur Bereitstellung von Informationen bei der Erhebung personenbezogener Daten in Bezug auf die betroffene Person aufgeführt. Die verantwortliche Person ist verpflichtet, unter anderem Auskunft über die Verantwortlichen, den Zweck der Verarbeitung und die Rechtsgrundlage, die Dauer der Speicherung sowie ihr Recht auf Zugang und Löschung der Daten zu geben. Verarbeitet die bearbeitende Person die Daten nachträglich zu einem anderen Zweck, ist diese verpflichtet, den Betroffenen vor Beginn der weiteren Bearbeitung über die weiteren Schritte zu informieren. Oft handelt es sich bei den ersten Informationen um eine Datenschutzerklärung. Anschließend kann der Verbraucher selbst entscheiden, ob er der Verwendung der Daten zustimmt oder widerspricht. Die Verarbeitung durch Big-Data-Analysen ist jedoch vielfältig und komplex, wodurch eine detaillierte Erklärung erforderlich ist, damit der Verbraucher

verständliche Informationen erhält (vgl. Scheuing, S., Datenschutz, 2015, S. 117). Daher hat das Europäische Parlament einheitliche Symbole veröffentlicht, um zu symbolisieren, was der Prozessor anschließend mit den Daten macht. Abbildung 1 zeigt diese sechs Symbole und ihre verschiedenen Bedeutungen. Das erste Symbol steht dafür, dass nur ein Minimum an persönlichen Daten benötigt wird, die für einen bestimmten Zweck benötigt werden. Das zweite Symbol zeigt, dass nur das Minimum an erforderlichen persönlichen Daten gespeichert ist. Das dritte Symbol zeigt, dass die persönlichen Daten nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Das vierte Symbol besagt, dass die gesammelten Daten nicht an Dritte weitergegeben werden. Die Tatsache, dass keine Daten verkauft oder ausgeliehen werden, ist durch das fünfte Symbol dargestellt. Das letzte Symbol der Abbildung zeigt an, dass keine personenbezogenen Daten unverschlüsselt aufbewahrt werden. Wenn diese Voraussetzungen erfüllt sind, kann in der hinteren Spalte ein grünes Symbol mit einem Haken eingefügt werden, ansonsten muss dort ein rotes X eingefügt werden (vgl. Europäisches Parlament, Symbole, 2013, S. 31).

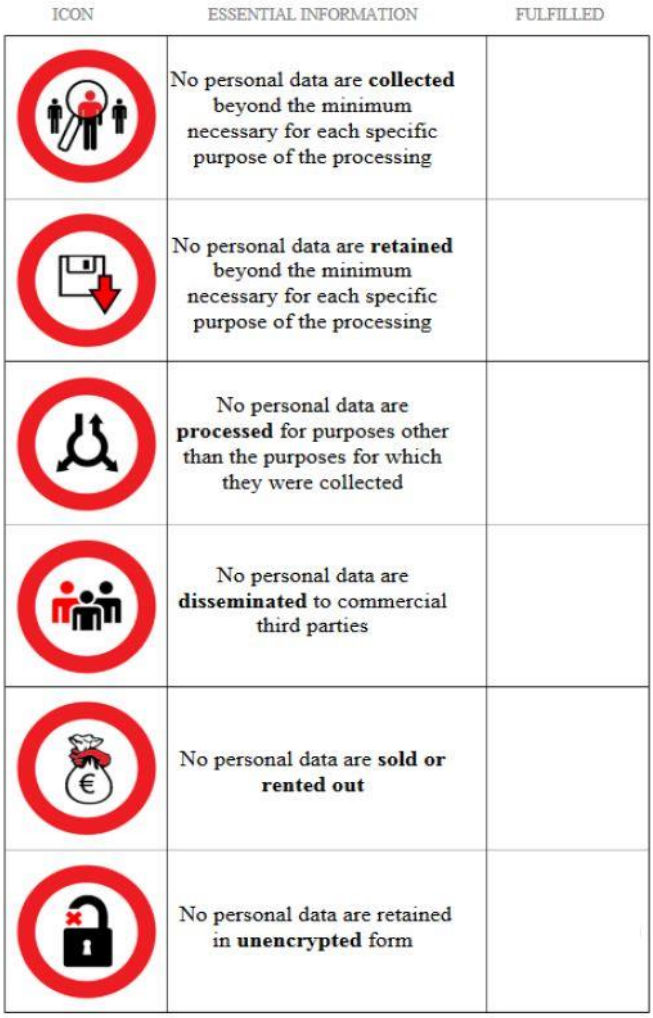


Abbildung 1: Standardisierte Bildsymbole des EU-Parlaments

Für den Verbraucher ist diese standardisierte Visualisierung von Datenschutzeinstellungen verständlicher und einfacher zu verstehen als eine Datenschutzerklärung und bietet einen klaren Überblick darüber, was danach mit ihren Daten geschieht (vgl. Raabe, O., Wagner, M., Big Data, 2018, S. 439).
Darüber hinaus hat jeder Verbraucher ein Recht auf Information. Zum Beispiel kann jeder Verbraucher eine Firma fragen, welche Daten über die Person gespeichert sind, und eine freie Kopie der relevanten persönlichen Daten muss zur Verfügung gestellt werden. Darüber hinaus muss es Auskunft über den Zweck der Verarbeitung, den Empfänger der Daten, die geplante Speicherdauer und das Recht zur Berichtigung oder Löschung dieser Daten geben (vgl. Scheuing S., Datenschutz, 2015, S. 117; Das europäische Parlament und der Rat der europäischen Union, DSGVO, 2016, Art. 15 Abs. 3 DSGVO). Artikel 12 der Verordnung legt sogar fest, dass Informationen klar und transparent und in einer klaren und einfachen Sprache zur Verfügung gestellt werden sollten. Da die Informationen innerhalb eines Monats nach Eingang des Ersuchens zur Verfügung gestellt werden müssen, wird dies eine Herausforderung für die Verwaltung der betreffenden Unternehmen, diese Frist nicht zu überschreiten. Nur bei einer großen Anzahl und komplexen Anwendungen ist es möglich, die Frist um zwei Monate zu verlängern. Dies muss jedoch der betroffenen Person innerhalb eines Monats unter Angabe von Gründen mitgeteilt werden.

4. Fazit

Obwohl der Begriff Big Data in der EU-Datenschutzverordnung nicht direkt erwähnt wird, verfolgt die Europäische Kommission das Ziel, Big Data mit dieser neuen Verordnung zu fördern und gleichzeitig die personenbezogenen Daten von EU-Bürgern zu schützen. Die Big-Data-Informationen und die damit verbundenen Anforderungen verbergen sich jedoch hinter dem Begriff Profiling, unter dem die Verordnung eine automatisierte Verarbeitung versteht, z.B. Big Data Analytics. Aus diesem Grund gibt es auch neue Anforderungen für Big-Data-Analysen. Den technischen und organisatorischen Maßnahmen, die eine Big-Data-Analyse ermöglichen soll, wird große Aufmerksamkeit geschenkt. Auf der anderen Seite sollte auch einen besseren Schutz personenbezogener Daten gewährleisten. Ein besonderes Augenmerk wird auf anonyme Daten gelegt, für die die EU-Datenschutz-Grundverordnung nicht gilt. Dabei ist jedoch im Einzelfall zu entscheiden, ob die Daten gemäß der Verordnung

als anonym zu klassifizieren sind, da ansonsten bestimmte zusätzliche Anforderungen zu erfüllen sind.

Die Verordnung lässt jedoch zwei Punkte offen. Zum einen, welche Qualität der Pseudonymisierung für einen ausreichenden Datenschutz erforderlich ist und ob personenbezogene Daten, die auch nach der Übermittlung an einen Bearbeiter verschlüsselt wurden, als personenbezogene Daten gelten, obwohl sie keinen Identifikationsschlüssel besitzen (vgl. Marnau, N., Pseudonymisierung, 2016, S. 431).

Positiv zu vermerken ist, dass das Europäische Parlament und der Rat der Europäischen Union erkannt haben, dass aufgrund der technologischen Entwicklungen in den letzten Jahren eine neue Datenschutzverordnung erforderlich ist, die ein einheitliches System für alle europäischen Mitgliedstaaten schafft. Dies kann sich positiv auf die Unternehmen auswirken, sobald die ersten Anstrengungen unternommen werden, da sie nur eine Regel einhalten müssen, auch wenn sie die Daten in verschiedenen Mitgliedstaaten verarbeiten.

In Deutschland treten die Bürger dieser Thematik nicht so positiv entgegentreten wie die Amerikaner. Vielen Unternehmen droht daher bei rechtswidrigem Verhalten ein Imageverlust. Darüber hinaus stellen Big-Data-Analysen einen großen Wert für Unternehmen dar und es drohen hohe Strafen, wenn die Regulierung außer Acht gelassen wird. Daher kann festgestellt werden, dass spätestens bis zum 25. Mai 2018 alle Big-Data-Analysen an die Vorschriften und Anforderungen der EU-Datenschutz-Grundverordnung angepasst werden müssen. Daher müssen die Unternehmen über ausreichend und speziell geschultes Personal für diese Probleme und Anforderungen verfügen. Außerdem muss, wie beschrieben, darauf geachtet werden, dass ein Bearbeiter ausgewählt wird, der die Vorschriften einhält (vgl. Duda, D., Dokumentationspflichten, 2017, S. 8).

Diese Seminararbeit befasst sich nur mit den Anforderungen der EU-Datenschutz-Grundverordnung für Big Data. Trotz des Ziels der Harmonisierung haben die EU-Mitgliedstaaten die Möglichkeit, Bestimmungen spezifischer zu machen.

Literaturverzeichnis

Das Europäische Parlament und der Rat der Europäischen Union, 2016: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016.

Duda, Daniela, 2017: Dokumentationspflichten der DS-GVO als Prüfgegenstand, in: Sowa, Aleksandra (Hrsg.), IT-Prüfung,Sicherheitsaudit und Datenschutzmodell, 2017, S. 7-22

Europäische Kommission, 2015: Fragen und Antworten - Datenschutzreform, http://europa.eu/rapid/press-release_MEMO-15-6385_de.htm, (Zugriff am 12.08.2018

Freiknecht, Jonas, 2014: Big Data in der Praxis, München: Carl Hanser Verlag, 2014

GfdS, 2013: GfdS wählt »GroKo« zum Wort des Jahres 2013, (13.12.2013), https://gfds.de/gfds-waehlt-groko-zum-wort-des-jahres-2013-2/, (Zugriff am 12.08.2018)

Grassegger, Hannes, Krogerus, Mikael, 2017: Ich habe nur gezeigt, dass es die Bombe gibt

Hagendorff, Thilo, 2017: Das Ende der Informationskontrolle. Bielefeld: transcript Verlag, 2017

Hornung, Gerrit, 2015: Datenschutzrechtliche Aspekte der Social Media, in: Hornung, Gerrit, Müller-Terpitz, Ralf (Hrsg.), Rechtshandbuch Social Media, 2015, S. 79-130

Kipker, Dennis-Kenji, 2015: Privacy by Default und Privacy by Design, in: Datenschutz und Datensicherheit - DuD, 39(6), S. 410–410

Marnau, Ninja, 2016: Anonymisierung, Pseudonymisierung und Transparenz für Big Data, in: Datenschutz Und Datensicherheit - DuD, 40(7), S. 428–433

Meier, Andreas, Kaufmann, Michael, 2016: SQL-& NoSQL Datenbanken,8. Aufl., Berlin: Springer, 2016

Nieendick, Michael, Jansen, Jochen, Kalinowski, 2018: Big Data Management auf Basis von In-Memory-Technologien, in: Keuper, Frank, Hamidian, Kiumars, Verwaayen, Eric, Kalinowski, Torsten, Kraijo, Christian (Hrsg.), Digitalisierung und Innovation, 2018, S. 242-265

Nitsch, Karl Wolfhart, 2017: Informatikrecht, 5. Aufl., Wiesbaden: Springer, 2017

Raabe, Oliver, Wagner, Manuela, 2018: Verantwortlicher Einsatz von Big Data, in: Datenschutz Und Datensicherheit - DuD, 227(7), S. 434–439

Roßnagel, Alexander, Geminn, Christian, Jandt, Silke, Richter, Philipp, 2016: Datenschutzrecht 2016 „Smart“ genug für die Zukunft?, Kassel: Kassel University Press GmbH, 2016

Scheuing, Sachiko, 2015: Offensive im Datenschutz, in: Schwarz, Thorsten (Hrsg.), Big Data im Marketing: Chancen und Möglichkeiten für eine effektive Kundenansprache, 2015, S. 115-125

Schwartmann, Rolf, Weiß, Steffen, 2017: Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz, 2017

Wrobel, Stefan, Voss, Hans, Köhler, Joachim, Beyer, Uwe, Auer, Sören, 2015: Big Data, Big Opportunities, in: Informatik-Spektrum, 38(5), S. 370–378

Anhang – Präsentation

EU-Datenschutz-Grundverordnung (DSGVO)
und die damit verbundenem Privatsphäre
im Internet

Kreativität und Technik
Andrea Hornik und Fabian Richter

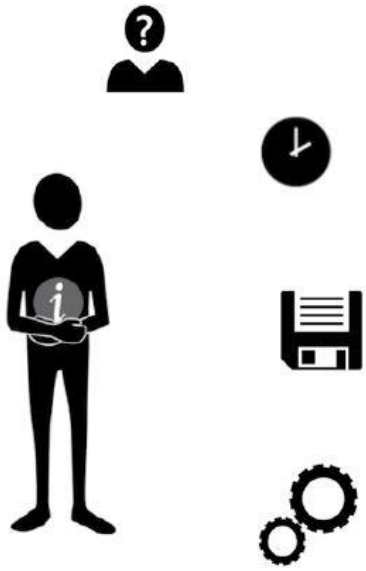
Agenda

1. Definition
2. Begriffliche Abgrenzung
3. Grundsätze
4. Inhalt
5. Privacy – Begriffe
6. Kritik
7. Reaktion
8. Diskussion

1

1. Definition

EU Datenschutz-Grundverordnung (DSGVO) kümmert sich um den Schutz der Daten von natürlichen Personen. Ziel ist das jede Person bestimmen kann, wer, wann und welche persönlichen Informationen über sie sammelt, speichert und verarbeitet. Dies gilt für alle EU-Unternehmen und jeden, der personenbezogene Daten von EU-Bürgern verarbeitet. Ziel dieser Verordnung ist die Harmonisierung von Datenschutzbestimmungen der EU und die stärkere Kontrolle von natürlichen Personen über eigene Daten.



2. Begriffliche Abgrenzung

DSGVO
Schutz von personenbezogenen Daten
BDSG & TMG (Telemediengesetz) unter einem einheitlichen Deckmantel

~

Informationssicherheit
Schutz aller Arten von Informationen vor Verlust, Diebstahl, Sabotage oder Missbrauch

v

3. Grundsätze

- Verbot mit Erlaubnisvorbehalt
  - Gesetzliche Erlaubnis
  - Erfüllung von Verträgen
  - Person hat ausdrücklich zugestimmt
- Zweckbindung
  - Nur für vorher definierten Zweck
- Speicherbegrenzung
  - Speicherung nur so lange wie sie wirklich benötigt werden
- Datenminimierung
  - Nur Informationen die auch wirklich für den Zweck benötigt werden
- Datenrichtigkeit & Datensicherheit
  - Recht auf Datenauskunft
  - Wann gelten Daten als genügend geschützt?

4. Inhalt

- Transparente Informationen
  - präzise, transparent, verständlich, leicht zugängliche Form, in einer klaren und einfachen Sprache
- Recht auf Vergessenwerden
- Recht auf Datenportabilität
- Rechenschaftspflicht
  - Dokumentation der Einhaltung der Datenschutzanforderungen, Sicherheitslecks
- Wie Einwilligung einholen?
  - schriftliche Dokumentation, Opt-In oder Opt-Out, Freiwillig

5. Privacy-Begriffe

- data protection by design
  - Datenschutz bereits bei Erarbeitung eines Datenverarbeitungsvorgangs technisch integriert
  - Beispiel: Pseudonymisierung
- data protection by default
  - Datenschutz bereits in den Voreinstellungen
  - „Privacy-Paradox“

6. Kritik

- Viele Aspekte in thematisiert
  - Beispiel: Grundsätze der DSGVO gegen BigData
  - Lösung durch Anonymisierung
    - erst der persönliche Bezug macht die Informationen wertvoll für die Auswertung
- Verordnung gilt für alle gleichermaßen
  - Unterschiedliche Ressourcen --> Benachteiligung
- Öffnungsklauseln unterminieren Datenschutz
- Überlastung der Unternehmen durch eine Flut von Auskunftsanforderungen
- Fotografie als personenbezogene Daten

7. Reaktionen

- Schließung und Beschränkung von Zugängen
  - Unsicherheit, Sanktionsfurcht, fehlende Vorbereitung
  - Beispiele:
    - Online-Spiele, Dienste und Medien des EU-Auslandes teils nicht mehr zugänglich
    - Websites, Blogs, Online-Shops im Inland geschlossen
    - Datenportabilität bei Musik-Streaming-Diensten mit Lücken