Datenschutz in der Industrie 4.0

Inhaltsverzeichnis

1. Aktuelle Situation

In der Heutigen Zeit macht gefühlt jedes dritte IT-Unternehmen Cloud-Produkte die mit „Künstliche Intelligenz“ aufgewertet werden, jedoch achtet kaum einer auf die Rechtlichen Voraussetzungen. Beispielsweise die sogenannte Künstliche Intelligenz (KI), dies sind Programme die anhand vergangener Daten Muster selbstständig erkennen sollen. Die dazu benötigten Datenmengen gehen dabei Erfahrungsgemäß von wenigen 10 Gigabyte(Zahlen oder Wörter) auf bis zu mehreren Terabyte(Bilderkennung). Ein weiteres Datenschutzrechtliches Minenfeld welches sich immer größerer Beliebtheit ist das verarbeiten von Daten auf Servern fremder Anbieter. Beispielsweise senden viele Elektroautos Daten an den Hersteller zu Telemetriezwecken[3, S. 172] oder die Standardmäßige Datensammlung von Windows 10, dort ist es zudem extrem Fraglich ob dieses Betriebssystem überhaupt in Bereichen, wo Persönliche Daten verarbeitet werden, eingesetzt werden darf. Die Datenschutz-Grundverordnung und das Bundesdatenschutzgesetz setzen dort Rechtliche Grenzen, die jedoch eher Abstrakt gehalten wurden. Und obwohl die Übergangsfrist im März endet haben viele Unternehmen noch keine Konsequenzen daraus gezogen.

2. Datenschutz-Grundverordnung

Die Datenschutz Grundverordnung (DSGVO) ist eine Verordnung der EU die Festlegt unter welchen Voraussetzungen Daten Verarbeitet werden dürfen. Personenbezogene Daten sind in der DSGVO Daten mit denen man unmittelbar einen Bezug zu einer Person herstellen kann. Diese Daten müssen Pseudonymisiert oder verschlüsselt werden um die Datensicherheit zu Gewährleisten. Die DSGVO definiert einige Vorschriften was das

Erheben, Verarbeiten und Speichern von Daten angeht, zu den wichtigsten gehören:

1. Zweckbindung, die Daten müssen einem Zweck dienen
2. Datenminimierung, Es dürfen nicht mehr Daten als Nötig gespeichert werden
3. Richtigkeit, es müssen Maßnahmen getroffen werden, mithilfe die Daten gelöscht werden können
4. Speicherbegrenzung, die Daten dürfen nur so lange gespeichert werden wie Nötig
5. Integrität und Vertraulichkeit, die Daten müssen durch Technische Maßnahmen geschützt werden

Zusätzlich stellt die DSGVO durch das Marktortsprinzip sicher, dass Unternehmen wie Google sich hier in Europa genauso an den Datenschutz halten müssen wie andere Firmen, weil nicht der Ort des Anbieters gilt, sondern der Ort wo Anbieter(Google, Facebook, etc.) und Nachfrager aufeinandertreffen. Zudem werden die Anforderungen an für die Einwilligung heruntergesetzt. Für nicht Personenbezogene Daten ist selbst eine stillschweigende Zustimmung erlaubt, dies ist aber zu Dokumentieren. Die Einwilligung für Personenbezogene Daten ist trotz dessen schriftlich zu erteilen. Die DSGVO definiert zudem Europaweit die Bedingungen für Datenschutzbeauftragter(Data Protection Officer), z. B. müssen Datenschutzbeauftragter (DSB) in jedem Fall eingestellt werden, wenn es sich um eine Öffentliche Stelle oder Behörde handelt, wenn die Verarbeitung von Daten eine umfangreiche oder systematische Überwachung erforderlich machen, oder umfangreich Personenbezogene Daten verarbeitet werden. Zudem ist er frühzeitig in die Verarbeitung von Personenbezogenen Daten Fragen eingebunden. Zur Erleichterung hat die DSGVO einige Dinge erlaubt mit denen betroffene Institutionen keine unnötigen Ausgaben tätigen müssen. Beispielsweise darf ein DSB für das Gesamte Unternehmen zuständig sein, anstatt für jede noch so kleine Außenstelle einen eigenen einzustellen. Voraussetzung ist, das der DSB von allen Niederlassungen gut erreichbar ist.

3. Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) regelt die Erhebung, Verarbeitung und die Nutzung von Personenbezogenen Daten. Das BDSG ist die nationale Umsetzung der ab 2018 anzuwendende Datenschutz-Grundverordnung. Als Personenbezogen werden Daten angesehen, wenn sie sachliche oder Persönliche Eigenschaften einer Natürlichen Person

bezeichnen, z. B. IP-Adresse, Telefonnummer oder eine Personalnummer. Diese Daten müssen entsprechend Geschützt gespeichert werden. Das BDSG arbeitet nach dem „Verbotsprinzip mit Erlaubnisvorbehalt“, daher ist die Erhebung, Nutzung und Verarbeitung verboten solange keine Erlaubnis eingeholt wurde oder durch ein Gesetz erlaubt ist. Einen Zusätzlichen Schutz haben Daten über die Ethnische Herkunft, politische Meinung, Religiöse oder Philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und das Sexualleben.

3.1. Verbraucherrechte

Das BDSG gibt Betroffenen grundsätzlich 4 Rechte zur Verfügung:

1. Auskunftsrecht
2. Korrekturrecht
3. Löschungsrecht

Das Auskunftsrecht[1] beschreibt, das das Betroffene über die Verarbeitung der Daten informiert werden müssen und gibt ihnen das Recht bei den Institutionen Anfragen zu den Gespeicherten Daten zu stellen. Das Recht auf Löschung(Recht auf Vergessen werden)[2], verpflichtet die Institution alle angegebenen Daten auf Anfrage zu Löschen, wenn unter anderem

- die Daten nicht mehr notwendig sind,
- die Einwilligung für die Datenverarbeitung widerruft oder keine Rechtsgrundlage mehr besteht oder
- Widerspruch gegen die Verarbeitung einlegt und es keine vorrangig berechtigte Gründe gibt.

4. Abkürzungen und Quellen

BDSG	Bundesdatenschutzgesetz
DPO	Data Protection Officer
DSB	Datenschutzbeauftragter
DSGVO	Datenschutz Grundverordnung
KI	Künstliche Intelligenz

Quellen

[1] Bundesrepublik Deutschland. *Auskunftsrecht der betroffenen Person*. Bundesdatenschutzgesetz §34. 2017.

[2] Bundesrepublik Deutschland. *Recht auf Löschung*. Bundesdatenschutzgesetz §35. 2017.

[3] Dieter Spaar. „Daten auf Rädern. Was moderne Autos speichern und wie man an die Informationen herankommt“. German.
In: *c't* 09 (09/2016 15. Apr. 2016), S. 170–172. ISSN: 0724-8679.