Datenschutz

Was ist Datenschutz?

Unter Datenschutz versteht man den Schutz personenbezogener Daten vor Missbrauch, oft im Zusammenhang auch mit dem Schutz der Privatsphäre. Zweck und Ziel im Datenschutz ist die Sicherung des Grundrechts auf informationelle Selbstbestimmung der Einzelperson. Jeder soll selbst bestimmen können, wem er wann welche seiner Daten und zu welchem Zweck zugänglich macht.

Datenschutz-Definition

Personenbezogene Daten sind gemäß Art. 4 Abs. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen „.

Das Gesetz sieht eine natürliche Person als identifizierbar an, „die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie“

* Namen
* einer Kennnummer
* Standortdaten
* einer Online-Kennung oder
* „einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“

Rechtsgrundlage im Datenschutz

Einer der Grundsätze der Datenschutz-Grundverordnung ist die rechtmäßige Verarbeitung personenbezogener Daten. Dafür muss immer eine Rechtsgrundlage zu deren Legitimation vorliegen. Je nach Zweck der Datenverarbeitung, kann der Verantwortliche die Rechtmäßigkeit dabei auf verschiedene Tatbestände stützen.

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ist in Art. 6 Abs. 1 DSGVO geregelt. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig,

wenn eine Einwilligung der betroffenen Person vorliegt,

zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen,

zur Erfüllung einer rechtlichen Verpflichtung

zum Schutze lebenswichtiger Interessen,

zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt oder

aufgrund einer Interessenabwägung erforderlich ist.

Die Datenverarbeitung ist bereits dann rechtmäßig, wenn einer der genannten Tatbestände vorliegt.

DSGVO

Zeitplan:

März 2016: offizielle deutsche Fassung der EU-DSGVO

April 2016: Beratung des EU-Ministerrats, danach Abstimmung im Europäischen Parlament

25. Mai 2018: Anwendbarkeit der EU-Datenschutz-Grundverordnung

Nach mehr als 4 Jahren Verhandlungszeit wurde die DSGVO vom Europäischen Parlament, dem Rat und der Kommission verabschiedet, um die folgenden Ziele zu erreichen:

Der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, soll gestärkt werden, insbesondere das Recht auf den Schutz personenbezogener Daten (Art. 1, Abs. 2 DSGVO).

Die Etablierung von verbindlichen Datenschutz-Standards in allen EU-Staaten vereinheitlicht das Datenschutzrecht innerhalb der EU.

Diese Vereinheitlichung erleichtert es den EU-Bürgern, die Kontrolle über ihre persönlichen Daten zu erlangen und auszuüben.

Die Standards schaffen außerdem eine verlässliche Rechtsgrundlage für den freien Verkehr personenbezogener Daten (Art. 1, Abs. 3 DSGVO).

Was ist Netzwerk-Sicherheit?

Netzwerksicherheit ist jede beliebige Aktivität, welche die Funktionsfähigkeit und Integrität Ihres Netzwerks und Ihrer Daten schützt.

Sie umfasst sowohl Hardware- als auch Softwaretechnologien

Sie hat eine Vielzahl von Bedrohungen zum Ziel

Sie hält die Bedrohungen davon ab, in Ihr Netzwerk einzudringen oder sich dort zu verbreiten

Eine effektive Netzwerksicherheit verwaltet den Zugriff auf das Netzwerk

Arten von Netzwerksicherheit

* Firewalls (basiert entweder auf Hardware, auf Software oder auf einer Kombination aus beidem)
* E-Mail-Sicherheit (Eine Anwendung für E-Mail-Sicherheit blockiert Angriffe und steuert ausgehende Nachrichten, um den Verlust vertraulicher Daten zu verhindern.)
* Antivirus- und Malwareschutz-Software (Die besten Malwareschutz-Programme scannen nicht nur Malware bei ihrem Eintreten, sondern verfolgen Dateien laufend nach, um Anomalien aufzuspüren, Malware zu entfernen und Schäden zu beheben.)
* Netzwerksegmentierung (Bei der softwaredefinierten Segmentierung wird der Netzwerkverkehr unterschiedlichen Klassifizierungen zugeordnet, wodurch die Durchsetzung von Sicherheitsrichtlinien erleichtert wird.)
* Zugriffskontrolle (Nicht jeder Benutzer sollte auf Ihr Netzwerk zugreifen können. Um potenzielle Angreifer fernzuhalten, müssen Sie jeden Benutzer und jedes Gerät kennen.)
* Usw.

3 Pfeiler der Netzwerksicherheit

Die Netzwerk-Sicherheit umfasst meist folgende drei Pfeiler: Authentizität, Vertraulichkeit und Integrität.

Bei der Authentizität der Kommunikationspartner geht es darum festzustellen, ob der Kommunikationspartner auch tatsächlich der ist, für den er sich ausgibt.

Bei der Vertraulichkeit einer Kommunikation geht es darum dafür zu sorgen, dass niemand Einblick in die Daten und Kommunikation erhält.

Zur Integrität zählen Mechanismen und Verfahren, die die Echtheit von Daten prüfen und sicherstellen können und somit auch vor Manipulation schützen.

Vereinfacht kann man sagen, dass es bei der Netzwerk-Sicherheit immer um die Authentifizierung der Kommunikationspartner und die Verschlüsselung der Kommunikation geht. Die Integrität ist in diesen Verfahren integriert und muss deshalb nicht explizit betrachtet werden.

Kann die Datensicherheit/Netzwerksicherheit dem Datenschutz schaden?

Grundsätzlich unterschützen, bis auf wenige Ausnahmen, die Maßnahmen, die zur Datensicherheit erfolgen, den Datenschutz.

-> Eine dieser Ausnahmen ist das Auslagern von Daten in eine Cloud. Kann das Auslagern in einen Cloud-Speicher die Daten vor Verlust schützen und ist grundsätzlich eher förderlich für die Datensicherheit, so verursacht diese Maßnahme in Hinblick auf den Datenschutz zahlreiche Risiken und Probleme. Bei einer Datensicherung in der Cloud, handelt es sich aus Datenschutzrecht bereits um eine Übermittlung, die wiederrum nur erlaubt ist, wenn sie auf einer Rechtsgrundlage oder einer informierten Einwilligung basiert. Hat der Cloud-Anbieter seinen Sitz zudem in einem Drittland, außerhalb der europäischen Union (EU) oder des europäischen Wirtschaftsraums (EWR), so muss die verantwortliche Stelle weitere Maßnahmen umsetzen, so ist üblicherweise ein angemessenes Datenschutzniveau herzustellen.

Möchte eine Organisation auf Cloud-Lösungen zurückgreifen, so ist ein deutscher bzw. europäischer Cloud-Anbieter und das Abschließen eines Vertrages zur Auftragsdatenverarbeitung (ADV) dringend anzuraten.

Hauptproblem: Der Nutzer

Das Hauptproblem ist der Nutzer

Das größte Sicherheitsproblem ist immer noch der Nutzer selbst. Die wichtigste Maßnahme ist die Sensibilisierung für Sicherheitsprobleme. Dadurch reduziert sich die Angriffsfläche automatisch.

Richtig böse ist es, wenn der Nutzer die Schadsoftware meist unwissentlich selbst installiert. Zum Beispiel durch das Öffnen eines E-Mail-Anhangs. Doch Otto-Normal-Nutzer ist sehr schwer von einem sehr vorsichtigen Umgang mit fremden Dateien zu überzeugen. Deshalb ist der Sicherheitsgewinn durch einen Virenscanner höher zu bewerten als die zusätzlich entstehende Angriffsfläche durch den Virenscanner selbst.

Doch Vorsicht, ein Virenscanner ist ein Tool zum Überprüfen von Dateien auf Schadsoftware. Mehr Sicherheit bietet er nicht. Er kommt immer nur dann zum Einsatz, wenn es eigentlich schon zu spät ist. Ein Virenscanner kann im Zweifelsfall den Virenbefall nicht verhindern, wenn er den Virus nicht kennt.

Was man wissen muss!

* Alles was wir über Sicherheit im Internet wissen kann man als überholt ansehen
* immer davon ausgehen, dass sich der Angreifer innerhalb der eigenen Organisation oder Netzwerk befindet
* interne Sicherheitsstrukturen so angelegen, dass der Zugang zu wichtigen Daten ständig kontrolliert wird
* Angriffe auf Sicherheitsverfahren werden immer besser.
* Ist man den Schwächen eines Verfahrens auf der Spur, dann dauert es nur noch wenige Jahre, bis jemand einen weiteren Trick findet

Unterschiede Datenschutz/Netzsicherheit

|  |  |
| --- | --- |
| Datenschutz | Netzwerksicherheit/Datensicherheit |
| - Schutz vor datenmissbrauch und -pannen (Grundsätze der Daten Sparsamkeit, Zweckbindung) | - Schutz von Daten |
| - Schutz personenbezogener daten | - Schutz aller Daten |
| - Schutz der informationellen Selbstbestimmung (Privatsphäre) | - Schutz vor Verlust, Zerstörung, Missbrauch, Zugriff durch Unberechtigte |
| - Gesetzliche vorschiften | - Technische Maßnahmen / Lösungen |
| - Theorie: beim Datenschutz wird der theoretische Ansatz „was soll erfüllt werden?“ verfolgt werden | - Praxis: Bei der Datensicherheit geht es unter anderem um die Umsetzung der Anforderungen des Datenschutzes, wobei der praktische Ansatz, „Was ist möglich?“, verfolgt wird. |

Datenschutz und Datensicherheit: Gemeinsamkeiten

- Schutz von Daten

- mit Daten muss vertraulich umgegangen werden

- es müssen Maßnahmen getroffen werden, um den Schutz zu gewährleisten

- Unternehmen muss Regelungen treffen, um beides gewährleisten zu können