HAMPP + PARTNER

Datenschutzgrundverordnung
Änderung bei der Verwendung personenbezogener Daten

Was ist die DSGVO?

DSGVO – EU 2016/679

- Verordnung beinhaltet den

… Schutz **natürlicher Personen** bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr…

- ist ab 25.05.2018 anzuwenden
- übergeordnetes Gesetz, löst Europäische Datenschutzrichtlinie, Bundesdatenschutzgesetz und alle weiteren gesetzlichen Normen bzgl. personenbezogener Daten ab

Folgen der DSGVO

- Vereinheitlichung des europäischen Datenschutzrechtes
- Keine Abminderung der Regelungen des DSGVO durch nationale Gesetze
- In vielen der 99 Artikel der DSGVO gibt es Öffnungsklauseln, die durch nationale Regelungen präzisiert werden können, jedoch keine Rechtssicherheit garantieren

Geltungsbereich der DSGVO

Nach Art. 3 DSGVO allgemein:
Die Verordnung findet Anwendung, wenn sich einer der Beteiligten in der EU oder in einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaates der EU unterliegt, befindet.

Erwägungsgrund 13 und 14 zur DSGVO zeigt folgende Einschränkungen:

- Die Verordnung enthält eine abweichende Regelung hinsichtlich des Führens eines Verzeichnisses für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen (Kleinstunternehmen sowie kleine und mittlere Unternehmen)
- Die Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen.

Was versteht die DSGVO unter „personenbezogenen Daten“?

Nach Art. 4 Nr. 1 DSGVO inhaltlich:
„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Was versteht die DSGVO unter „Verarbeitung“?

Nach Art. 4 Nr. 2 und 4 DSGVO inhaltlich:
„Verarbeitung“ bedeutet jeden, mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Dies beinhaltet insbesondere die automatisierte Verarbeitung personenbezogener Daten zur Analyse und Vorhersagung persönlicher Indikatoren wie wirtschaftliche Situation, persönliche Vorlieben, Verhalten, Interessen, gesundheitlichem Zustand, etc..

Wann dürfen personenbezogene Daten verarbeitet werden?

Verbotsprinzip mit Erlaubnisvorbehalt
D.h., dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Prinzip verboten ist.
Sie ist nur dann erlaubt, wenn:

- die betroffene Person ausdrücklich ihre Zustimmung zur Erhebung, Verarbeitung und Nutzung gegeben hat,
- eine klare Rechtsgrundlage gegeben ist,
- die Daten anonymisiert sind,
- Behörden einen offiziellen Auftrag ausführen,
- andere Ausnahmen (Strafverfolgung, etc.) gegeben sind.

Was wird gefordert?

- technische und organisatorische Maßnahmen (toM´s) zum Schutz personenbezogener Daten von außen und innerhalb des Unternehmens, incl. genehmigte Verhaltensregeln
- ein Verfahren, mit dem toM´s überprüft, bewertet und beurteilt werden
- Dokumentations- und Nachweispflicht von Verfahren und Maßnahmen durch ein Verarbeitungsverzeichnis (v.a. Vertraulichkeit, Integrität, Verfügbarkeit, Rechtmäßigkeit, Transparenz, Zweckgebundenheit, Datensparsamkeit…)

Welche Herausforderung bringt die DSGVO mit sich?

- Beweislastumkehr: der Verantwortliche muss beweisen, dass er ordnungsgemäß gehandelt hat (unabhängig von einem Schadenseintritt)
- Vorgaben der DSGVO zur Beweisführung:
  - Geschäftsprozessbeschreibung
  - Verarbeitungsverzeichnis
  - Datenschutz-Folgeabschätzung
  - genehmigte Verhaltensregeln oder Zertifizierung nach ISO 27001
- regelmäßige Überprüfung der Software zur privacy by design (Datenschutz durch Technikgestaltung) und privacy by default (Datenschutz durch datenschutzfreundliche Voreinstellung)
- Prüfung alle Altdatenbestände auf Konformität mit der DSGVO

Wie kann man die Forderungen umsetzen und welchen Nutzen kann man daraus ziehen?

Es gibt mehrere Wege, die Anforderungen der DSGVO umzusetzen, z.B.:

- erweiterte Einführung eines Informations-Sicherheits-Management-Systems (ISMS nach ISO 27001)

  Ein integriertes ISMS zur Kombination von Datenschutz mit Informationssicherheit. Somit werden nicht nur personenbezogene Daten, sondern auch alle anderen Firmendaten, wie Finanz-, Forschungs-, Prozessdaten, etc. als schutzbedürftig erachtet.

- Datenschutz in Verbindung mit BSI-Grundschutz (auch in Verbindung mit ISMS nach ISO 27001 möglich)

  Gestaltung der erforderlichen Maßnahmen der DSGVO mit Hilfe der Standards des Bundesamt für Sicherheit in der Informationstechnik (BSI) zum IT-Grundschutz. Dies beinhaltet Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen zu unterschiedlichen Aspekten der Informationssicherheit.

- Individuelle Lösungen:

  Risikoanalyse, Maßnahmeregelungen, Verarbeitungsverzeichnisse, Prozessbeschreibungen, Datenschutz-Folgeabschätzungen, Verhaltensregelungen stellen die Voraussetzungen zum Grundschutz personenbezogener Daten dar und können in separaten Prozessen abgebildet werden.

Machen Sie Ihr Unternehmen sicher!
Wir unterstützen Sie gern.

Hampp + Partner GmbH
König-Wilhelm-Straße 41
74360 Ilsfeld

Telefon: +49 (0) 70 62 / 6 29 33
E-Mail: info@hampp-partner.de
www.hampp-partner.de

AO 22.02.2018