Datenschutz und -sicherheit

Im E-Commerce – kurz und kompakt in Stichpunkten

Datenschutz

Aus dem Recht auf Selbstbestimmung und der Würde des Menschen resultiert der Datenschutz, festgeschrieben in der Datenschutzgrundverordnung (DSVGO) in Kraft seit dem 25 Mai 2018 und umgesetzt im BDSG-neu.

- Die Datenschutzerklärung muss jederzeit direkt aufrufbar sein[1]
- Setzt an, bevor die Informationen überhaupt vorliegen

Arten von Daten[2]

personenbezogenen Daten

- Beschreiben eine natürliche Person
- Beispiele: Name, Geburtsdatum, Adresse, Bankdaten, IP-Adressen, Cookies, Geschlecht etc.

Besonders personenbezogene Daten

Ethnische und kulturelle Herkunft, alle politischen, religiösen und philosophischen Ansichten, genetische und biometrische Daten wie Fingerabdruck, Venen oder Iris.

anonymisierter Daten

Sie sind kein Problem und werden z. B. für ein allgemeines Nutzerprofils der Website benutzt. Das Geschlecht, die Altersspanne, die Region, die Interessen etc.

pseudoanonymisierte Daten

- Ein Datensatz mit ID ohne Verbindung zum echten Datensatz
- Grauzone, wegen möglicher Zuweisbarkeit durch Zusammensetzung Merkmalen
- Hinweis auf Erhebung und Recht des Widerspruches

Grundsätze[3]

Verbot mit Erlaubnisvorbehalt

- Generelles Verbot der Datenerhebung mit gesetzlichen Ausnahmen
- Daten nach Ablauf der Notwendigkeit direkt löschen
- Ausgenommen sind aufbewahrungspflichtige Daten

Zweckbindung

- Erhebung ausschließlich für die vertraglich festgehaltenen Bedingungen (den Zweck) erlaubt
- unmittelbar danach Löschungspflichtig
- Weitergabe an Dritte verboten
- Ausgenommen für die Strafverfolgung, und Abrechnung

[1] Vgl. Impressum und Datenschutz-Ausführungen auf einer Website unterbringen (datenschutz.org)
[2] Vgl. Personenbezogene Daten – Definition und Beispiele (ionos.de) und Datenschutz im E-Commerce | Rechtssicher gemäß DSGVO (ionos.de)
[3] Vgl. Datenschutz im Unternehmen inkl. Checkliste (datenschutz.org)

Datenminimierung

Es dürfen auch nur die für den Zweck benötigten Daten verlangt werden.

Transparenz und Hinweispflicht

- leicht verständliche Sprache
- Aufzählung aller Daten nach Art, Umfang und Verwendung
- Datenschutzeinwilligung[4] der Nutzer vor außerrechtlicher Datenerhebung
- Möglichkeit jederzeit zu widersprechen
- Alle Datenschutzmaßnahmen müssen im sog. Verarbeitungsverzeichnis dokumentiert werden

Vertraulichkeit

- Schutz vor Verarbeitung, Veränderung, Vernichtung oder Diebstahl anderer, technisch und organisatorisch
- keine klaren Handlungsempfehlungen der DSVGO
- mehr Schutz ist immer besser
- Im Zweifel entscheidet ein Gericht, ob die ergriffenen Maßnahmen ausreichend waren

Meldepflicht[5]

Datenpannen müssen innerhalb von 72 Stunden nachdem sie dem Unternehmen auffallen an die Betroffenen und die zuständige Behörde gemeldet werden.

Kopplungsverbot

Unternehmen dürfen Leistungen nicht mit der Einwilligung zur Abgabe von Daten, die für die Leistung nicht erforderlich sind, verpflichten.

Strafen[6]

- bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes
- Ordnungswidrige Handlungen, die absichtlich, vorsätzlich oder fahrlässig …:
  - den Absender oder den kommerziellen Charakter einer Nachricht verschleiern,
  - den Nutzer nur unvollständig oder gar nicht über die Art der Datenerfassung informieren,
  - gegen die gesetzlichen Bestimmungen personenbezogene Daten erheben, verarbeiten, speichern oder nicht rechtzeitig löschen oder
  - ein Nutzungsprofil mit Daten über den Träger des Pseudonyms zusammenführen.

Rechte der Nutzer[7]

- Schadensersatzansprüche
- Auch Betroffenenrechte genannt
- Auskunftsrecht
- Recht auf Vergessenwerden (Löschungsrecht)
- Berichtigungsrecht
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Recht auf Einschränkung der Verarbeitung

[4] Vgl. DSGVO Zusammenfassung 2020: Datenschutz-Grundverordnung für Webseitenbetreiber (ionos.de)
[5] Vgl. Datenpanne melden | Compiliance (haufen.de)
[6] Vgl. Datenschutz im E-Commerce | Rechtssicher gemäß DSGVO (ionos.de)
[7] Vgl. Betroffenenrechte in der Datenschutz-Grundverordnung (datenschutz-praxis.de)

Auftragsverarbeitung[8]

- externes Unternehmen verarbeitet Daten des Nutzers
- Verantwortung liegt beim Webseitenbetreiber
- Vertrag über die Verarbeitung und Übertragung
- Genaueres in Art. 28 geregelt wie
  - Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten.

Datensicherheit[9]

- wie die Daten geschützt werden
- alle Daten werden geschützt
- Vertraulichkeit
- Integrität
- Verfügbarkeit durch „Data Loss Prevention (DLP)“[10]

Prinzipien

- „Privacy by Design“
  - Datenschutz von Anfang an mit einbauen
  - Mit möglichst wenig Daten auskommen können
- „Privacy by Default“
  - Datenschutz freundlichste Einstellung als Standard
- Datenschutz-Folgeabschätzung (DSFA)[11]
  - Risiko-Abschätzung
  - Besonderer Schutz
    - Im Cloud-Computing
    - Bei medizinischen Daten

TOM[12]

- Technische und organisatorische Maßnahmen

Unterschied

Technische Maßnahmen	Organisatorische Maßnahmen

- bauliche Maßnahmen
  o Umzäunung des Geländes
  o Sicherung von Türen und Fenstern
  o Alarmanlagen
- Soft- und hardware-Maßnahmen wie
  o Benutzerkonto
  o Passworterzwingung
  o Logging (Protokolldateien)
  o biometrische Benutzeridentifikation
	- Handlungsanweisungen, Verfahrens- und Vorgehensweisen umgesetzt
	  o Besucheranmeldung
	  o Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
	  o Vier-Augen-Prinzip
	  o festgelegte Intervalle zur Stichprobenprüfungen

[8] Vgl. Datenschutz in der Auftragsdatenverarbeitung - Überblick der Pflichten (mein-Datenschutzbeauftragter.de)
[9] Vgl. Datensicherheit: Was bedeutet das? (Datenschutz.org)
[10] Vgl. Probleme mit der Datensicherheit (e-commerce-Magazin.de)
[11] Vgl. Datenschutz im E-Commerce | Rechtssicher gemäß DSGVO (ionos.de)
[12] Vgl. Technische und Organisatorische Maßnahmen (datenschutz-wiki.de)

Schutzmaßnahmenkategorien

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügsbarkeitskontrolle
- Trennungsgebot

Handlungsempfehlungen

Clients

- Keine garantierte Sicherheit
- Geringste Datenpreisgabe
- 2 E-Mailkonten (ein privates und seriöses sowie einen für alle anderen Dienste)
- Jeder Dienst ein anderes zufälliges min. 12 Zeichen langes Passwort
- Abhilfe kann ein Passwortmanager bieten
- Sichere Verbindung
  - SSL
  - W-Lan
  - DNS-Anbieter
- Aktuelle Software
  - Betriebssystem
  - Browser (Negativbeispiel: Internet Explorer[13])
- Trackingblocker wie UBlockOrigin

Server

- Aktuelle Software
  - Betriebssystem (z. B. Debian Buster)
  - Webserver (z. B. Apache 2.4)
  - Programmiersprachen (z. B. PHP 7.4.1)
  - Datenbank (z. B. MariaDB 10.4)
- ‚Best Practice' beim Programmieren
  - Sorgfältig, klar strukturiert lassen Sicherheitslücken einfacher finden (z. B. MVC-Model)
  - IDE weißt auf veraltete Techniken hin
  - Gegen die einfachsten Angriffe rüsten wie SQL-Injection
- Sich selbst angreifen
- Backups
- Offene Ports schließen[14]

Literaturverzeichnis

Betroffenenrechte in der Datenschutz-Grundverordnung. (27. September 2016). Abgerufen am 02. Februar 2020 von Datenschutz-Praxis.de: https://www.datenschutz-praxis.de/fachartikel/betroffenenrechte-in-der-datenschutz-grundverordnung/

Datenschutz im E-Commerce | Rechtssicher gemäß DSGVO. (24. Januar 2019). Abgerufen am 28. Januar 2020 von ionos.de: https://www.ionos.de/digitalguide/websites/online-recht/datenschutz-im-e-commerce/

Datenschutz im Unternehmen (inkl. Checkliste). (24. Mai 2018). Abgerufen am 28. Januar 2020 von Datenschutz.org: https://www.datenschutz.org/unternehmen/

Datenschutz in der Auftragsdatenverarbeitung - Überblick der Pflichten. (kein Datum). Abgerufen am 07. Februar 2020 von Mein-Datenschutzbeauftrager.de: https://www.mein-datenschutzbeauftragter.de/auftragsverarbeitung/

Datensicherheit: Was bedeutet das? (24. Mai 2018). Abgerufen am 23. Januar 2020 von Datenschutz.org: https://www.datenschutz.org/datensicherheit-massnahmen/

[13] Vgl. Internet Explorer: Kritische Sicherheitslücke entdeckt (techbook.de) und vgl. Internet Explorer: Microsoft warnt vor kritischer Sicherheitslücke... (t3n.de)

[14] Datensicherheit von Online-Shops als eines der Top-Themen 2017 (techdision)

DSGVO Zusammenfassung 2020: Datenschutz-Grundverordnung für Webseitenbetreiber. (05. Februar 20202). Abgerufen am 05. Februar 2020 von Digital Guide IONOS by 1&1: https://www.ionos.de/digitalguide/websites/online-recht/datenschutz-grundverordnung-regeln-fuer-unternehmen/

FAQ zur Datenschutz-Grundverordnung im E-Commerce. (26. Januar 2018). Abgerufen am 02. Februar 2020 von it-recht-kanzlei.de: https://www.it-recht-kanzlei.de/fragen-antworten-datenschutz-grundverordnung-e-commerce.html

Impressum und Datenschutz-Ausfürhugnen auf einer Website unterbringen. (11. Juli 2018). Abgerufen am 28. Januar 2020 von Datenschutz.org: https://www.datenschutz.org/impressum-datenschutz/

Internet Explorer: Kritische Sicherheitslücke endeckt. (14. November 2019). Abgerufen am 04. Februar 2020 von techbook.de: https://www.techbook.de/easylife/web/internet-explorer-sicherheitsluecke

Kleibl, J. (02. Februar 2020). *Internet Explorer: Microsoft warnt vor kritischer Sicherheitslücke...* Von t3n.de: https://t3n.de/news/internet-explorer-microsoft-1201437/ abgerufen

Personenbezogene Daten - Definition und Beispiele. (15. Juni 2018). Abgerufen am 30. Januar 2020 von Digital Guide IONOS by 1&1: https://www.ionos.de/digitalguide/websites/online-recht/personenbezogene-daten/

Probleme mit der Datensicherheit. (09. Juni 2011). Abgerufen am 08. Februar 2020 von e-Commerce-Magazin.de: https://www.e-commerce-magazin.de/probleme-mit-der-datensicherheit/

Rehm, S.-M. (30. April 2019). *Datenpanne melden | Compiliance*. Abgerufen am 05. Februar 2020 von haufen.de: https://www.haufe.de/datenpanne-melden_230130_483940.html

So gehen sie richtig mit Auskunftsersuchen um. (26. Oktober 2018). Abgerufen am 02. Februar 2020 von Datenschutz-Parxis.de: https://www.datenschutz-praxis.de/fachartikel/so-gehen-sie-richtig-mit-auskunftsersuchen-um/

Technische und organisatorische Maßnahmen. (11. September 2018). Abgerufen am 23. 01 2020 von Datenschutz-wiki.de: https://www.datenschutz-wiki.de/Technische_und_organisatorische_Maßnahmen

Willkommer, J. (11. Januar 2017). *Datensicherheit von Online-Shops als eines der Top-Themen...* Abgerufen am 02. Februar 2020 von techdivision: https://www.techdivision.com/blog/datensicherheit-von-online-shops-als-eines-der-top-themen-2017.html