FRT CONSULT GMBH
IT Dienstleistungen & Business Dienstleistungen

frtpartner

Telefon: 09221 / 900 - 0
Telefax: 09221 / 900 - 111
Kontakt: info@frtconsult.de
Adresse: Kurt-Schumacher-Str. 23
95326 Kulmbach

Datenschutz-Newsletter 2024 / I

Aktuelles rund um den Datenschutz

Neue Verordnung der EU: der Data Act

Auswertungen von Daten haben ein hohes Innovationspotential, da sie als wesentliche Ressource für die Sicherung des digitalen Wandels eingeordnet werden. Die EU-Datenstrategie hat sich daher zum Ziel gesetzt, Hürden bei der optimalen Verteilung von Daten abzubauen. Es sollen Datensilos aufgebrochen und sowohl Verbrauchern als auch Unternehmen Zugang zu Daten verschafft werden. Dazu wurde der Data Act vom Europäischen Parlament verabschiedet. Am 11. Januar 2024 ist die neue Verordnung in Kraft getreten. Sie findet sowohl auf personenbezogene als auch auf nichtpersonenbezogene Daten Anwendung und ist nach einer Übergangsfrist ab dem 12. September 2025 unionsweit anwendbar.

Der Data Act sieht folgende Datenzugangs- und Datennutzugsrechte vor. Diejenigen, die Daten durch die Nutzung von vernetzten Produkten oder verbundenen Diensten erzeugen, sollen Zugang zu diesen Daten erhalten und sie darüber hinaus an Dritte weitergeben können. Betroffen sind zum Beispiel Nutzer von vernetzten Haushalts- und Fitnessgeräten und Industriemaschinen (IoT-Geräte), aber auch mit Produkten verknüpfte Steuerungssoftware mittels der die Funktionalität des Produkts aus der Ferne gesteuert werden kann. Darüber hinaus wurden Regelungen zur Schaffung von offenen und interoperablen Schnittstellen zum Datenaustausch geschaffen.

Zugangsbeschränkung bestehen durch die Vorgaben der DSGVO, sofern es sich bei den angeforderten Daten um personenbezogene Daten handelt, die nicht vom Nutzer selbst stammen.

Künstliche Intelligenz (KI) und Datenschutz

Durch den Einsatz von KI wird das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts gefährdet. Es entsteht ein Konflikt zwischen KI und Datenschutz, der Wettbewerbsfähigkeit der Unternehmen und der Sicherheit der Bürger und ihrer Daten.

Bei der Benutzung von Large Language Models wie ChatGPT ergeben sich datenschutzrechtliche Probleme. Es können personenbezogene Daten eingegeben werden, sodass auch die generierten Antworten solche enthalten können. Für diese Verarbeitung liegt oft keine Rechtsgrundlage vor, da der Betroffene zuvor keine Einwilligung erteilt hat. Nach Artikel 6 Abs. 1 lit. f DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eins Dritten erforderlich ist und solange die Interessen

oder Grundrechte der betroffenen Personen nicht überwiegen.

Um Large Language Models wie ChatGPT datenschutzkonform nutzen zu können, sollten Unternehmen gemäß dem Bayerischen Landesamt für Datenschutzaufsicht einige grundlegende Regeln beachten:

- Die Gesetzmäßigkeit der Verarbeitung muss sichergestellt sein.
- Es muss ein Auftragsverarbeitungsvertrag abgeschlossen werden.
- Es sollte eine Datenschutzfolgenabschätzung durchgeführt werden.
- Der Dienst sollte in der Datenschutzerklärung aufgeführt werden.
- Die eingegebenen Daten sollten vollständig protokolliert werden.
- Es sollten angemessene technische und organisatorische Maßnahmen umgesetzt werden.
- Der generierte Text sollte abgeändert bzw. paraphrasiert werden und nicht wörtlich übernommen werden, um Urheberrechts- und Markenverletzungen zu vermeiden.
- Die Regeln zur Nutzung von künstlichen Intelligenzen sollten im Arbeitsvertrag stehen.
- Es sollte die Datenschutzrichtlinie des Dienstes bekannt sein, um die Art und Weise, wie die Daten verwendet werden, zu kennen.
- Unternehmen müssen ihren Informationspflichten aus Art. 13, 14 DSGVO und dem Transparenzgebot nachkommen. Es muss festgehalten werden, welche Daten tatsächlich verarbeitet werden und ob und an wen eine Weitergabe erfolgt.

Datenschutzrisiko Fax

Der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit macht aktuell darauf aufmerksam, dass das Fax in verschiedener Hinsicht datenschutzrechtlich problematisch ist.

Zum einen kann von dem Versender als Empfänger nur schwer sichergestellt werden, dass das Fax beim Empfänger aufgrund mangelnder Zugriffsbeschränkungen nicht in die Hände von unbefugten Dritten gelangt.

Des Weiteren sind Faxe grundsätzlich nicht verschlüsselt.

Fazit: Vorzuziehen ist eine E-Mail mit einem verschlüsselten Anhang ober bei noch höherem Schutzbedarf eine E-Mail mit Ende-zu-Ende Verschlüsselung.

Der Landesbeauftragte weist aber auch darauf hin, dass zum Beispiel in medizinischen Fällen im Rahmen der Risikoabwägung der Schutz der Gesundheit und die Sicherung von Leib und Leben überwiegen könne mit der Folge, dass in dringenden Einzelfällen aus Sicht des Datenschutzes eine Übermittlung per Fax legitim sein könne.

Stand: 20. März 2024

Alle Beiträge sind nach bestem Wissen zusammengestellt. Eine Haftung für deren Inhalt kann jedoch nicht übernommen werden. Für Fragen zum Thema Datenschutz stehen Ihnen unsere zertifizierten Datenschutzbeauftragten gerne zur Verfügung.

Thomas Hesz, RA/StB; Marcel Peetz (M.Acc.), WP/StB/FBIStR; Maria Gayer, RAin; Stefan Gräbe
Zertifizierte Datenschutzbeauftragte (TÜV)
Telefon: 09221 / 900 - 0
edsb@frtconsult.de www.frtpartner.de