Datenschutz-Verordnung

Sparfuch

Schweiz - wollerauerstrasse 31 – 8834 schindellegi

Letzte Aktualisierung:	24/06/2023

Definitionen

Unterehmen	Sparfuch, ein Unternehmen registriert, unter der Nummer CH130.1.030.590-7
DSG	Datenschutzgesetz 2018, das die Datenschutzverordnung der EU umsetzt. GDSG - 25. Mai 2018
Verantwortliche Person	**Dario Zúger**
Systemverzeichnis	Ein Verzeichnis aller Systeme oder Kontexte, in denen personenbezogene Daten von der Organisation verarbeitet werden.

1. Welche personenbezogenen Daten ("Ihre personenbezogenen Daten") werden von uns erfasst?

Daten, die Sie ("Sie", "Ihre") während des Bewerbungsprozesses eingeben, Anhänge, Antworten auf Screening-Fragen.

Ihre IP-Adresse.

Ihre Anmeldedaten (E-Mail-Adresse und verschlüsseltes Passwort)

Cookies, die es uns ermöglichen zu erfahren, wie unsere Kursangebote genutzt werden. 2. Grundsätze des Datenschutzes

Die Organisation verpflichtet sich, die Daten gemäß ihrer Verantwortung im Rahmen des Datenschutzgesetzes zu verarbeiten.

Die DPA-Anforderungen für personenbezogene Daten sind:

a. rechtmäßig, nach Treu und Glauben und auf transparente Weise in Bezug auf Einzelpersonen verarbeitet werden.

b. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist; die Weiterverarbeitung zu Archivierungszwecken im öffentlichen Interesse, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gilt nicht als unvereinbar mit den ursprünglichen Zwecken.

c. angemessen und sachdienlich sein und sich auf das beschränken, was im Hinblick auf die Zwecke, für die sie verarbeitet werden, erforderlich ist.

d. sachlich richtig und, soweit erforderlich, auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke, für die sie verarbeitet werden, unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

e. in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht, und zwar nicht länger, als es für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger aufbewahrt werden, sofern die personenbezogenen Daten ausschließlich für im öffentlichen Interesse liegende Archivierungszwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke verarbeitet werden, sofern die geeigneten technischen und organisatorischen Maßnahmen ergriffen werden, die nach dem DSG erforderlich sind, um die Rechte und Freiheiten natürlicher Personen zu schützen; und

f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Beschädigung, unter Verwendung geeigneter technischer oder organisatorischer Maßnahmen."

3. **Allgemeine Bestimmungen**

a. Diese Richtlinie gilt für alle personenbezogenen Daten, die von der Organisation verarbeitet werden.

b. Die verantwortliche Person trägt die Verantwortung für die ständige Einhaltung dieser Richtlinie durch die Organisation.

c. Diese Richtlinie wird mindestens einmal jährlich überprüft.

d. Die Organisation muss sich beim Information Commissioner's Office als Organisation, die personenbezogene Daten verarbeitet, registrieren lassen.

4. **Rechtmäßige, faire und transparente Verarbeitung**

   a. Um sicherzustellen, dass die Verarbeitung von Daten rechtmäßig, fair und transparent ist, führt die Organisation ein Systemregister.

   b. Das Register der Systeme wird mindestens einmal jährlich überprüft.

5. **Rechtmäßige Zwecke**

   a. Alle von der Organisation verarbeiteten Daten müssen auf einer der folgenden Rechtsgrundlagen beruhen: Einwilligung, Vertrag, rechtliche Verpflichtung, lebenswichtige Interessen, öffentliche Aufgabe oder berechtigte Interessen.

   b. Die Organisation vermerkt die entsprechende Rechtsgrundlage im Register der Systeme. c. Wird die Einwilligung als Rechtsgrundlage für die Datenverarbeitung herangezogen, so ist der Nachweis der Einwilligung zusammen mit den personenbezogenen Daten aufbewahrt werden.

   c. Der Einzelne hat das Recht auf Zugang zu seinen personenbezogenen Daten, und alle an die Organisation gerichteten Anfragen werden zeitnah bearbeitet.

   d. Werden Mitteilungen an Einzelpersonen auf der Grundlage ihrer Zustimmung versandt, so sollte die Möglichkeit des Widerrufs der Zustimmung eindeutig gegeben sein, und es sollten Systeme vorhanden sein, die sicherstellen, dass ein solcher Widerruf in den Systemen der Organisation korrekt wiedergegeben wird.

6. **Datenminimierung**

   a. Die Organisation stellt sicher, dass personenbezogene Daten den Zwecken entsprechen, für die sie verarbeitet werden, dafür erheblich sind und sich auf das beschränken, was im Hinblick auf die Zwecke, für die sie verarbeitet werden, erforderlich ist.

7. **Genauigkeit**

   a. Die Organisation ergreift angemessene Maßnahmen, um die Richtigkeit der personenbezogenen Daten zu gewährleisten.

   b. Soweit es für die Rechtsgrundlage, auf der die Daten verarbeitet werden, erforderlich ist, werden Maßnahmen ergriffen, um sicherzustellen, dass die personenbezogenen Daten auf dem neuesten Stand gehalten werden.

8. **Archivierung / Entfernung**

a. Um sicherzustellen, dass personenbezogene Daten nicht länger als nötig aufbewahrt werden, führt die Organisation eine Archivierung Politik für jeden Bereich ein, in dem personenbezogene Daten verarbeitet werden, und überprüft diesen Prozess zweimal im Jahr.

b. In der Archivierung Politik ist zu berücksichtigen, welche Daten wie lange und warum aufbewahrt werden sollen/müssen.

9. **Sicherheit**

a. Die Organisation stellt sicher, dass personenbezogene Daten sicher gespeichert werden, indem sie moderne Software verwendet, die auf dem neuesten Stand gehalten wird.

b. Der Zugriff auf personenbezogene Daten ist auf das Personal zu beschränken, das den Zugriff benötigt, und es sollten angemessene Sicherheitsvorkehrungen getroffen werden, um eine unbefugte Weitergabe von Informationen zu verhindern.

c. Wenn personenbezogene Daten gelöscht werden, sollte dies auf sichere Weise geschehen, so dass die Daten nicht wiederherstellbar sind.

d. Geeignete Lösungen für die Sicherung und Wiederherstellung im Katastrophenfall müssen vorhanden sein.

10. **Verstoß**

Im Falle einer Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Weitergabe von oder zum Zugriff auf personenbezogene Daten führt, bewertet die Organisation unverzüglich das Risiko für die Rechte und Freiheiten von Personen und meldet diese Verletzung gegebenenfalls dem ICO (weitere Informationen auf der ICO-Website). (https://ico.org.uk)

ENDE DER VERORDNUNG