Datenschutz - Leitfaden

Inhaltsverzeichnis

Vorwort Seite 3

Begriffe Seite 3

Personenbezogene Daten Seite 3

Verarbeitung von Daten Seite 3

Betroffene Seite 4

Grundsätze Seite 4

Transparenz Seite 4

Vertraulichkeit und Datensicherheit Seite 4

Zweckmäßigkeit Seite 4

Die Datenverarbeitung Seite 4

Vertraulichkeit der Verarbeitung Seite 4

Sicherheit der Verarbeitung Seite 5

Pflege des Datenbestandes Seite 5

Datenverarbeitung für Vertragsverhältnisse Seite 5

Datenverarbeitung aufgrund gesetzlicher Erlaubnis und aufgrund eines berechtigten Interesses Seite 5

Mitarbeiterdaten Seite 5

Rechte von Betroffenen Seite 6

Datenschutzaudits Seite 6

Verantwortlichkeiten und Sanktionen Seite 6

Vorwort

Ziel dieses Leitfadens ist, die Bedeutung und die Wichtigkeit des gesetzlichen Datenschutzes zu veranschaulichen und für alle interessierten Parteien (Kunden, Lieferanten, Mitarbeiter usw.) zu verdeutlichen, wie die Putenzucht Miko mit dem Thema Datenschutz und der Umsetzung der Datenschutzgrundverordnung umgeht.

Die Putenzucht Miko verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung des gesetzlichen Datenschutzes. Dieser Leitfaden gilt für alle Standorte und Unternehmensbereiche.

Datenschutz ist für uns nicht nur die Einhaltung der gesetzlichen Bedingungen, sondern ist Teil unsers Selbstverständnisses und unserer Firmenphilosophie.

Datenschutz ist in der Verantwortung der Geschäftsführung.

Begriffe

1. Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die es ermöglichen eine natürliche oder juristische Person zu identifizieren. Dies kann nicht nur direkt (Name etc.) erfolgen, sondern auch indirekt durch die Beschreibung eindeutiger Merkmale erfolgen.

Beispiele:

- Name, Adresse, Geburtsdatum
- Foto, Fingerabdrücke, biometrische Daten
- Bankdaten, Kennwörter, KFZ-Kennzeichen, IP-Adressen
- Indirekte Beschreibung z.B. „die Geschäftsführung der Putenzucht Miko“
- Und vieles mehr

2. Verarbeitung von Daten

Unter Verarbeitung versteht man jedes Erfassen, Ordnen, Speichern, Aufbewahren, Anpassen, Abfragen, Übermitteln, Verwenden, Löschen etc. von Daten. Damit ist sowohl die Verarbeitung mittels EDV als auch Bearbeitung in Papierform gemeint. Daten können erst dann nicht mehr verarbeitet werden, wenn diese unwiederbringlich gelöscht oder vernichtet worden sind.

3. *Betroffene*

Als Betroffener gilt jeder, dessen personenbezogene Daten in jeder denkbaren Form verarbeitet werden.

Grundsätze

1. *Transparenz*

Jeder Betroffene muss bzw. kann über den Umgang mit seinen Daten informiert werden. Alle Daten sind nicht über Dritte, sondern direkt beim Betroffenen nachzufragen.

Für jeden Betroffenen bleibt erkennbar, zu welchem Zweck, in welcher Form, in welchem Umfang und mit welchen Aufbewahrungsfristen seine Daten verarbeitet werden.

2. *Vertraulichkeit und Datensicherheit*

Es werden alle organisatorische und technische Möglichkeiten gegen unberechtigte Verwendung, gegen unberechtigte Zugriffe und Weitergabe sowie gegen Verlust, Diebstahl und Zerstörung getroffen.

3. *Zweckmäßigkeit*

Personenbezogene Daten werden nur für die festgelegten und legitimierten Zwecke erhoben und verarbeitet. Vor jeder Verarbeitung personenbezogener Daten muss der notwendige Umfang ermittelt und berücksichtigt werden. Es werden keine Daten nur für zukünftige Zwecke auf Vorrat aufbewahrt.

Die Datenverarbeitung

1. *Vertraulichkeit der Verarbeitung*

Personenbezogene Daten unterliegen dem Datengeheimnis. Den Mitarbeitern ist jede unbefugte Nutzung, Weitergabe oder Verwendung (also jede Verwendung die außerhalb der in diesem Leitfaden beschriebenen Möglichkeiten ist) untersagt. Dies erfordert auch eine definierte Aufgabenbeschreibung für jeden Mitarbeiter.

2. Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unrechtmäßige Verwendung und Verarbeitung, gegen unzulässige Zugriffe, gegen Verlust oder Diebstahl sowie gegen Vernichtung und Verfälschung zu schützen.

Daten in Papierform sind entsprechend gesichert und versperrt aufzubewahren. Elektronische Daten sind nach dem jeweils neuesten Stand der Technik abzuspeichern und zu sichern. Es sind alle technischen und organisatorischen Maßnahmen zur Sicherheit der Aufbewahrung zu treffen.

3. Pflege des Datenbestandes

Die Aktualität des Datenbestandes ist laufend zu überprüfen. Nicht mehr zutreffende, nicht mehr benötigte, unvollständige oder veraltete Daten werden gelöscht bzw. entsprechend archiviert. Zur Pflege des Datenbestandes wird ein(e) zuständige(r) ernannt. Unter „Löschen“ ist die vollständige Vernichtung zu verstehen (mechanische Vernichtung bei Daten in Papierform). Temporär nicht benötigte Daten werden in der EDV auf „inaktiv“ gesetzt. Bei Daten in Papierform sind diese entsprechend unzugänglich zu lagern.

4. Datenverarbeitung für Vertragsverhältnisse

Daten, welche für die Geschäftsabwicklung mit Kunden und Lieferanten notwendig sind, werden nur im dafür notwendigen Ausmaß verwendet, verwaltet und aufbewahrt. Zugang zu diesen Kunden- und Lieferantendaten haben nur mit der jeweiligen Auftragsart befasste MitarbeiterInnen. Die Aufbewahrungszeit richtet sich nach den gesetzlichen Fristen (7 Jahre) bzw. nach internen Vorgaben (3 Jahre für Daten mit Relevanz für unser Qualitätsmanagementsystem). Die Kundendateien werden auch darüber hinaus aufbewahrt, um diese im Bedarfsfall (z.B. für Folgeaufträge) verfügbar zu haben.

5. Datenverarbeitung aufgrund gesetzlicher Erlaubnis und aufgrund eines berechtigten Interesses

Die Verarbeitung von Daten, ist auch zulässig, wenn gesetzliche Vorschriften diese notwendig machen. Ebenso ist die Verarbeitung von Daten aufgrund eines berechtigten Interesses zulässig (z.B. Durchsetzung von offenen Forderungen).

6. Mitarbeiterdaten

Daten von Mitarbeitern dürfen nur in dem Ausmaß verwendet werden, das für die Anbahnung, die Begründung, die Durchführung und die Beendigung des Arbeitsverhältnisses notwendig ist.

Daten von Bewerbern sind nach der Ablehnung der Bewerbung zu löschen, es sei denn, der Bewerber hat dazu eingewilligt, dass seine Daten in Evidenz behalten werden können. Bei sogenannten „Blindbewerbungen“ kann von einer solchen Einwilligung ausgegangen werden.

Besonders schutzwürdige Daten (Religionszugehörigkeit, Gesundheitsdaten, Mitgliedschaft in Gewerkschaften oder politischen Parteien, gerichtliche Verurteilungen, anhängige Exekutionsverfahren etc.) sind als solche entsprechend vertraulich zu behandeln.

7. Rechte der Betroffenen

Ein Betroffener kann Auskunft darüber verlangen, welche personenbezogenen Daten, zu welchem Zweck und in welcher Form aufbewahrt und verwendet werden. Ein Betroffener kann die Berichtigung, die Ergänzung oder die Löschung seiner personenbezogenen Daten verlangen. Die Löschung kann nur für jene Art der Verarbeitung verlangt werden, die außerhalb der zulässigen Verwendung liegt.

8. Datenschutzaudits

Im Rahmen der laufenden und jährlichen QM-Audits sind alle datenschutzrelevanten Bereiche zu überprüfen. Dazu gehören insbesondere organisatorische und technische Maßnahmen zur Datensicherheit.

9. Verantwortlichkeiten und Sanktionen

Für die rechtskonforme Verarbeitung, Verwendung und Sicherung personenbezogener Daten ist die Geschäftsleitung verantwortlich.

Die Geschäftsleitung stellt sicher, dass die Mitarbeiter im Umgang mit personenbezogenen Daten geschult sind, dass im Betriebsablauf eine ordnungsgemäße und rechtskonforme Datenverarbeitung sichergestellt ist und dass Verstöße gemeldet werden.

Jeder Mitarbeiter ist verpflichtet unbefugte oder unrechtmäßige Verarbeitung, Vernichtung, Verlust, Veränderung, Weitergabe an Dritte etc. der Geschäftsleitung zu melden.

Eine Nichteinhaltung durch einzelne Mitarbeiter kann zu arbeitsrechtlichen Konsequenzen führen.

Frankenburg, am 22. Mai 2018

_____

Wolfgang Miko

Geschäftsführer