Risikoanalyse mit dem VKKT-Modell

“

Unter einer Risikoanalyse kann sich zwar jeder etwas vorstellen, aber dennoch ist dieser Begriff recht pauschal und in der Praxis kommt schnell die Frage auf: "Wie genau gehe ich denn nun vor?" Das potenzielle Risiko eines Verarbeitungsvorgangs ist immer anhand einer objektiven Bewertung zu beurteilen. Risiken können grundsätzlich entweder durch Handlungen von Menschen oder durch die Natur begründet sein. Natürliche Risiken wären beispielsweise Erdbeben, Blitzeinschläge, Hochwasser usw. Ein Risiko durch Menschen kann sowohl durch Mitarbeiter oder auch durch externe Dritte wie z.B. Dienstleister gegeben sein. In beiden Fällen kann ein Schaden absichtlich oder aus Versehen verursacht werden. Diese Arten von Risiken gilt es prinzipiell zu unterscheiden und vor allem in seine Überlegungen zur Risikoanalyse mit einzubeziehen. Zum besseren Verständnis lässt sich das am sogenannten VKKT-Modell erläutern. Das steht für Vogel, Katze, Käfig, Tür. Man muss sich hierbei nämlich einen Vogel vorstellen, der in einem Käfig mit einer Tür sitzt, vor dem eine Katze lauert. Hierbei ist der Vogel das Schutzobjekt, der Käfig die Schutzmaßnahme, die Katze die Bedrohung und die Tür des Käfigs die Sicherheitslücke. Der Vogel steht hier im übertragenen Sinne für personenbezogene Daten, die das primäre Schutzobjekt im Sinne der Datenschutzgrundverordnung darstellen. Es gilt nun also das Schutzobjekt vor der Bedrohung zu schützen. Es gibt zwar eine grundsätzlich wirksame Schutzmaßnahme, hier den Vogelkäfig, die hat jedoch eine potenzielle Sicherheitslücke, nämlich die Tür. Abhängig davon, wie sensibel bzw. wie wertvoll das Schutzobjekt ist, in dem Beispiel also der Vogel und wie die konkreten Bedrohungen aussehen, müssen die Schutzmaßnahmen gewählt und deren möglichen Sicherheitslücken beseitigt werden. In diesem Beispiel könnte man für einen sehr wertvollen Vogel beispielsweise eine organisatorische Maßnahme treffen. Es kann z.B. eine Arbeitsanweisung erlassen werden, durch die sichergestellt wird, dass die Käfigtür niemals unverschlossen gelassen wird, damit die Katze nicht an den Vogel kommt. Auch könnte ein besserer Käfig gekauft werden, der dann als technische Maßnahme sicherstellt, dass sich Tür immer selbstständig schließt, oder es wird ein extra Mitarbeiter dafür abgestellt, dessen Aufgabe es ist, den Vogel vor der Katze zu schützen. Ist der Vogel nicht ganz so wertvoll bzw. nicht so wichtig für seinen Besitzer, könnte man auch das Sicherheitsrisiko durch die Katze in Kauf nehmen und sich im Falle des Verlustes des Vogels einfach einen neuen zulegen. Was dieses vergleichsweise simple Beispiel zeigen soll, ist der Umstand, dass es in jedem Unternehmen zu einer individuellen Ermittlung und Einstufung der vorhandenen personenbezogenen Daten sowie zur Identifizierung bestehender Risiken und letztlich auch zur Umsetzung von angemessenen Sicherungsmaßnahmen kommen muss. Welche Maßnahmen nun genau zum Einsatz kommen, wird durch die DSGVO nicht vorgegeben. Sie müssen aber für das individuelle Risiko angemessen sein. Unter dem Strich stehen verschiedene Reaktionsmöglichkeiten zur Verfügung: Minderung des Risikos, Behandlung des Risikos, Vermeidung des Risikos, auch Übertragung des Risikos auf Dritte oder auch die Akzeptanz des Risikos. Wenn man diese Möglichkeiten anhand des VKKT-Beispiels betrachtet, ließen sich also beispielsweise Personen abstellen, die für die Beobachtung und eventuelle Ablenkung der Katze vom Vogel verantwortlich sind, Risikominderung. Die Katze aus dem Raum mit dem Vogelkäfig aussperren, Risikobehandlung. Den Vogel abschaffen, Risikovermeidung, oder eine "Tierversicherung" für den Vogel abschließen, die Risikoübertragung. Außerdem bleibt noch die Möglichkeit, gar nichts zu ändern und die Bedrohung des Vogels durch die Katze einfach hinzunehmen, Risikoakzeptanz. Etwa weil der Schadenseintritt als sehr unwahrscheinlich eingestuft wird und man im Falle eines Falles dann eben einen neuen Vogel kauft. Natürlich hinkt hier der Vergleich, aber es wird auf jeden Fall deutlich, was die einzelnen Optionen bewirken sollen. Außerdem wird klar, dass jede Maßnahme individuell auf die jeweiligen Unternehmen und auf das erkannte Risiko abgestimmt werden muss. Entscheidend ist dabei natürlich, dass man sich überhaupt Gedanken dazu macht und die Risiken für die eigenen Datenverarbeitungsvorgänge identifiziert. In einem zweiten Schritt müssten dann Gegenmaßnahmen erdacht und umgesetzt werden. Zu guter Letzt verlangt die DSGVO auch eine Dokumentation darüber, um im Zweifelsfall seiner Nachweispflicht nachkommen zu können.

