

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

DSGVO

Risikostufen

Die Datenschutz-Grundverordnung (DSGVO) verlangt, dass sowohl Verantwortliche als auch Auftragsverarbeiter die von ihnen ergriffenen Maßnahmen zur Umsetzung datenschutzrechtlicher Bestimmungen risikobasiert ausrichten, um betroffene Personen angemessen zu schützen (Art. 24 Abs. 1 DSGVO). Folglich ist das zentral zu berücksichtigende Risiko nach DSGVO das Risiko für die Rechte und Freiheiten betroffener Personen, nicht aber Risiken für den Verantwortlichen oder Auftragsverarbeiter.

Um das Risiko zu beurteilen, das für betroffene Personen mit einer personenbezogenen Datenverarbeitung einhergeht, ist eine Risikoanalyse erforderlich, die wiederum über das Maß der von einem Verantwortlichen und/oder Auftragsverarbeiter zu treffenden Schutzmaßnahmen entscheidet. Die DSGVO kennt zwei Risikostufen, nämlich „Risiko“ und „hohes Risiko“ (u. a. Art. 33, 34 DSGVO). Ergänzend zu diesen Risikostufen wird auch der Ausdruck „voraussichtlich nicht zu einem Risiko“ führend verwendet (Art. 27 Abs. 2 lit. a und Art. 33 Abs. 1 DSGVO). Eine vollständige risikofreie Verarbeitung personenbezogener Daten wird allerdings als nicht möglich angesehen.

Auf dieser Grundlage lässt sich eine differenzierte Risikoabstufung im Rahmen der Risikobeurteilung in
- „geringes Risiko“,
- „Risiko“ und
- „hohes Risiko“

vornehmen (DSK Kurzpapier Nr. 18, S.2).

Zu möglichen Risiken für betroffene Personen, zählen physische, materielle oder immaterielle Schäden für betroffene Personen, wie etwa der Verlust der Kontrolle über personenbezogene Daten, Einschränkungen ihrer Rechte, Diskriminierung oder Identitätsdiebstahl bzw. -betrug (Erwgr. 85 DSGVO).

Die DSGVO legt nicht fest, wann welche Risikostufe (also z. B. ein „hohes Risiko“) erreicht wird. Sie verlangt jedoch, dass Risiken anhand ihrer Eintrittswahrscheinlichkeit und Schwere sowie ggf. auf Grundlage (weiterer) objektiver Kriterien bewertet und einer der entsprechenden Risikostufe zugeordnet werden (DSK Kurzpapier Nr. 18, S.4). Diese Bewertung hat unter Berücksichtigung möglicher Folgeschäden sowie Art, Umfang, Umständen und Zweck der Verarbeitung zu erfolgen (Erwgr. 76 DSGVO). Dadurch kann auch ein Vorfall von geringer Schwere, aber hoher Eintrittswahrscheinlichkeit in eine höhere Risikokategorie einzuordnen sein.

Kontakt
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Annika.Selzer@sit.fraunhofer.de
06151 869 100
Autorin: Luisa Hehn--Mark

Die vorliegenden Ergebnisse sind im Rahmen des Fraunhofer Heilbronn Forschungs- und Innovationszentrums Cybersicherheit, das durch die Dieter Schwarz Stiftung gefördert wird, entstanden.
Die hier enthaltenen Informationen sind sorgfältig erstellt worden, können eine Rechtsberatung jedoch nicht ersetzen. Eine Haftung oder Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird daher nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse/Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.