CANTON DU VALAIS
KANTON WALLIS

Préposé cantonal à la protection des données et à la transparence
Kantonaler Datenschutz- und Öffentlichkeitsbeauftragter
Lauris Loat

Merkblatt zur Datenschutz-Folgenabschätzung (DSFA) im Sinne von Artikel 30b GIDA

1. Anwendungsbereich des Merkblatts zur DSFA

Das vorliegende Merkblatt richtet sich an die Behörden des Kantons Wallis im Sinne von Art. 3 Abs. 1 GIDA in ihrer Eigenschaft als Verantwortliche für die Bearbeitung von Personendaten.

2. Gegenstand und Zweck der DSFA

Seit dem 1. Januar 2024 muss gemäss Art. 30b GIDA für jede geplante Datenbearbeitung, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, eine DSFA erstellt werden.

Als Arbeitsinstrument des modernen Datenschutzrechts zielt die DSFA darauf ab, die Rechte der betroffenen Personen in der sozialen Realität der Digitalisierung sicherzustellen. Die DSFA betrifft daher sowohl neue Bearbeitungen von Personendaten als auch die Weiterentwicklung oder Erweiterung einer vorbestehenden Datenbearbeitung.

Zweck einer DSFA ist es, bereits im Vorfeld die mit einem Projekt verbundenen hohen Risiken zu identifizieren, die sich durch ihre Eintrittswahrscheinlichkeit und – aufgrund der Einstufung als «hoch» – durch die Schwere ihrer Auswirkungen auszeichnen.

Die DSFA beschränkt sich nicht nur auf die Voraussehbarkeit und Bewertung hoher Risiken. Ihr praktischer Nutzen liegt vielmehr auch darin, die Herleitung und Analyse systemischer und sicherheitstechnischer Risiken nachvollziehbar zu dokumentieren und durch geeignete Massnahmen auf ein datenschutzrechtlich vertretbares Niveau zu reduzieren.

3. Schutz der DSFA

Gemäss Art. 30b GIDA müssen die vom Gesetz erfassten hohen Risiken die Persönlichkeit oder die Grundrechte der betroffenen Person bedrohen. Der Persönlichkeitsschutz ist somit als wesentliches Schutzobjekt des Datenschutzes zu verstehen, aus dem sich als primäre Schutzobjekte der DSFA die Privatsphäre und die informationelle Selbstbestimmung ableiten lassen.

Werden Personendaten rechtswidrig bearbeitet, kann dies physische und finanzielle Folgeverletzungen nach sich ziehen, die neben den primären Schutzobjekten des Datenschutzes auch andere Rechtsgüter oder Grundrechte wie das Recht auf Leben, auf körperliche Unversehrtheit oder auf Eigentum tangieren. Solche Verletzungen können die von der Bearbeitung betroffenen Personen aber auch, im weiteren Kausalverlauf, die Verantwortlichen für die Datenbearbeitung betreffen.

In Anbetracht dieser Risikokategorisierung wird dem Verantwortlichen für die Datenbearbeitung empfohlen, die Evaluation des hohen Risikos in zwei Schritten vorzunehmen:

- In einem ersten Schritt werden die Risiken für die primären Schutzobjekte der Privatsphäre und der informationellen Selbstbestimmung der betroffenen Personen bewertet;
- In einem weiteren Schritt werden die Folgerisiken für die übrigen Rechtsgüter und Grundrechte (Recht auf Leben, physische Unversehrtheit, Eigentum, usw.) bewertet.

4. Bewertung des hohen Risikos

Avenue de l'Industrie 8, CH-1870 Monthey
Tel +41 (0)27 607 18 70 e-mail: prepose@admin.vs.ch

Das Vorliegen eines hohen Risikos ergibt sich gemäss Art. 30b Abs. 2 GIDA aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Das Gesetz enthält eine nicht abschliessende Aufzählung von Beispielen, bei denen ein hohes Risiko vorliegt:

- bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;
- bei einem Profiling;
- wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

Aufgrund seiner Auslegungsbedürftigkeit eröffnet der unbestimmte Gesetzesbegriff des hohen Risikos den Verantwortlichen für die Datenbearbeitung wie auch der Datenschutzaufsicht, welche durch den kantonalen Beauftragten ausgeübt wird, einen weiten Anwendungsspielraum. Die Definition dieses Begriffs wird im Laufe der Zeit durch die Praxis und die Rechtsprechung präzisiert werden.

Unter die Art einer Bearbeitung, die ein hohes Risiko mit sich bringen kann, fallen beispielsweise das Profiling im Sinne von Art. 3 Abs. 8 GIDA, das eine Bewertung der wesentlichen Aspekte der Persönlichkeit einer natürlichen Person erlaubt sowie andere Formen der automatisierten Datenbearbeitung, wie die automatisierte Einzelentscheidung im Sinne von Art. 20 GIDA. Zu den Umständen einer Bearbeitung zählen beispielsweise das Subordinationsverhältnis zwischen dem Verantwortlichen für die Datenbearbeitung und den betroffenen Personen.

5. Risikovorprüfung

Ist davon auszugehen, dass eine geplante Bearbeitung mit potenziell hohen Risiken verbunden ist, muss der Verantwortliche für die Datenbearbeitung eine (summarische) Vorprüfung der mit dem Projekt verbundenen Risiken durchführen. Die Vorprüfung muss die in Art. 30b Abs. 3 GIDA genannten Kriterien erfüllen, welche für die DSFA selbst gelten.

Die Vorprüfung ist so früh wie möglich, d.h. bereits in der Projektplanung vorzunehmen, auch wenn die Einzelheiten der Bearbeitung noch nicht festgelegt sind. Es kann daher empfehlenswert sein, mehrere Varianten vorzusehen.

Der Verantwortliche für die Datenbearbeitung muss das Ergebnis der Vorprüfung sowie seine Schlussfolgerungen dokumentieren. Sollte das Ergebnis nicht eindeutig ausfallen, empfiehlt es sich, eine DSFA durchzuführen.

6. Pflicht zur Durchführung einer DSFA

Hat die Vorprüfung ergeben, dass eine geplante Datenbearbeitung mit einem potenziell hohen Risiko verbunden sein könnte, so muss eine DSFA erstellt werden. Angesichts der Vorgaben von Art. 18 GIDA (Datenschutz durch Technikgestaltung und durch Voreinstellung) muss sie, wie schon die Vorprüfung, so früh wie möglich durchgeführt werden. Angesichts der Tatsache, dass zu diesem Zeitpunkt üblicherweise noch zahlreiche Einzelheiten geregelt werden müssen, bietet es sich wie bei der Vorprüfung an, mehrere Varianten zu erarbeiten, die im Laufe des Prozesses angepasst und sortiert werden.

Nach Art. 30b Abs. 3 GIDA muss eine DSFA Folgendes enthalten:

- eine Beschreibung der geplanten Bearbeitung;
- eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person;
- die vorgesehenen Massnahmen zum Schutz der Persönlichkeit und der Grundrechte der betroffenen Person.

Werden Personendaten ins Ausland übermittelt, muss die Übermittlung selbst im Rahmen der DSFA geprüft werden. Gerade wenn das Empfängerland nicht über ein angemessenes Datenschutzniveau verfügt, können potenziell hohe Risiken auftreten, auf die der Verantwortliche

für die Datenbearbeitung mangels materieller sowie rechtlicher Einflussmöglichkeiten keinen Einfluss nehmen kann. In einer solchen Konstellation wird die DSFA ergeben, dass ein hohes Restrisiko besteht. Darüber hinaus muss die DSFA darauf hinweisen, dass eine zuverlässige Bewertung dieser Risiken nicht möglich ist. Diese Anforderung kann je nach Wirksamkeit der getroffenen technischen, rechtlichen und organisatorischen Massnahmen insbesondere dann relevant sein, wenn Personendaten in Rechenzentren ausgelagert werden sollen, deren Betreiber zu einem Konzern gehört, der seinen Sitz in einem Staat hat, dessen Rechtsordnung kein vergleichbares Datenschutzniveau wie dasjenige der Schweiz bietet.

Im Rahmen der DSFA muss der Verantwortliche für die Datenbearbeitung geeignete Massnahmen zum Schutz der Persönlichkeit und der Grundrechte der betroffenen Personen vorsehen, um die anfänglich hohen Risiken auf ein angemessenes Niveau zu reduzieren. Die geplanten Massnahmen können eine Interessenabwägung zwischen den Interessen der betroffenen Person und denen des Verantwortlichen für die Datenbearbeitung beinhalten. Daher müssen sie in der DSFA hinreichend begründet werden.

7. Hohes Restrisiko

Nach Abschluss der DSFA kann trotz der vom Verantwortlichen für die Datenbearbeitung geplanten Massnahmen ein hohes Risiko bestehen bleiben.

In einem solchen Fall muss der kantonale Datenschutz- und Öffentlichkeitsbeauftragte vorgängig informiert werden (Art. 30b Abs. 4 GIDA). Der Beauftragte hat dann eine Frist von zwei Monaten, um Einwände gegen die geplante Datenbearbeitung zu erheben und geeignete Massnahmen vorzuschlagen. Dieser Punkt sollte unbedingt im Rahmen der Projektentwicklung mitberücksichtigt werden, damit nicht vergessen geht, dass die Entwicklung des Projekts aufgrund der vorherigen Konsultation des Beauftragten länger dauern kann.

In diesem Zusammenhang überprüft der Beauftragte, ob die ihm vorgelegte DSFA die identifizierten hohen Restrisiken deutlich, verständlich und präzise ausweist. Er prüft auch, ob die geplante Datenbearbeitung angesichts der Risiken mit den Anforderungen der Datenschutzgesetzgebung vereinbar ist und ob sie für die betroffenen Personen als zumutbar erscheint und daher sowohl im Hinblick auf den erwarteten Umfang als auch auf die erwartete Intensität vertretbar ist. Die Stellungnahme des Beauftragten kann sich auf die vorgesehene Datenbearbeitung oder die Struktur der DSFA beziehen, z.B. wenn der Verantwortliche für die Datenbearbeitung unmittelbare Risiken nicht richtig bewertet oder ausgewiesen hat.