Datenschutzhinweis Datenschutzfolgeabschätzung

nach Artikel 35 DSGVO

Wann ist diese notwendig?

Wie geht man vor?

Ein Service des DRV-Ausschusses Datenschutz

Berlin, Mai 2019

DIE REISEWIRTSCHAFT
Alle Ziele. Eine Stimme.

1. Grundsätzliches

Was ist mit der Datenschutzfolgeabschätzung gemeint?

Die Datenschutzfolgeabschätzung (nachfolgend „DSFA“ abgekürzt) ist im Prinzip eine Risikoabwägung bei der Verarbeitung von personenbezogenen Daten. Sie stellt ein – gesetzlich vorgeschriebenes – Instrument dar, das Risiko bei der Verarbeitung von personenbezogenen Daten in einem großen Umfang oder mit einem erheblichen Ausmaß für die Betroffenen, auf die Rechtmäßigkeit der Datenverarbeitung vorab und laufend zu überprüfen.

In welchen Fällen ist eine DSFA notwendig?

Eine DSFA ist nicht bei jeder Datenverarbeitung vorgeschrieben.

Eine DSFA muss dann vor Beginn der geplanten Verarbeitung von personenbezogenen Daten vorgenommen werden, wenn die

„...*Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung* ***voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen*** *zur Folge…*“

hat (vgl. Art. 35 Abs. 1 DSGVO).

Wichtig: Auch Klein-Unternehmen, die keinen Datenschutzbeauftragten bestellen müssen, können verpflichtet sein, eine DSFA vorzunehmen!

Wann liegt dann ein solches „hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ vor?

Das ist genau die kritische Frage, die sich jedes Unternehmen, also jeder datenschutzrechtlich Verantwortliche vor der Datenverarbeitung stellen muss.

Eine DSFA ist insbesondere in folgenden Fällen erforderlich (Art. 35 Abs. 3 DSGVO):

a) **systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen**, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) **umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten** gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische **umfangreiche Überwachung öffentlich** zugänglicher Bereiche;

2. Die Bedeutung der "DSFA – MUSS – LISTE"

Da die vorstehend genannten Kriterien, wann eine DSFT durchgeführt werden muss, sehr allgemein gehalten sind und in der Praxis schwierig abzugrenzen sind, legen die Aufsichtsbehörden in einer sog. „MUSS-Liste" die Arten von Datenverarbeitungen fest, bei denen zwingend eine DSFA vorab stattfinden muss.

Diese MUSS-Liste ist aus zweierlei Gründen für die Mitgliedsunternehmen sehr wichtig:

1. Soweit eine geplante Datenverarbeitung im Unternehmen Gegenstand der MUSS-Liste ist, muss eben auch die DSFA vorab erfolgen und dokumentiert werden, da andernfalls ein Bußgeld bis zu 10 Mio. Euro oder 2% vom weltweiten Gesamtumsatz droht.

2. Die MUSS-Liste ist aber auch für alle anderen Datenverarbeitungsvorgänge, die nicht ausdrücklich aufgeführt sind, eine wichtige Orientierungshilfe zur Abwägung, ob eine DSFA stattfinden muss oder nicht.

3. Vorsicht Falle! Die Tatsache, dass eine bestimmte Datenverarbeitung nicht auf der MUSS-Liste genannt ist, bedeutet keinen Freibrief, dass eine DSFA nicht erfolgen müsste: Es muss nur dann individuell geprüft werden.

Diese MUSS-Liste wird, gerade seit Einführung der DSGVO von den Aufsichtsbehörden regelmäßig aktualisiert und von der Datenschutz-konferenz der Aufsichtsbehörden in Deutschland (kurz „DSK") veröffentlicht.

Aktuell findet sich die Liste auf der Seite der DSK unter den Anwendungshinweisen:

https://www.datenschutzkonferenz-online.de/anwendungshinweise.html

Das bei Veröffentlichung aktuellste Dokument in der Version 1.1 hat folgenden etwas kryptischen Link:

https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf

Darüber hinaus veröffentlichen teilweise die einzelnen Aufsichtsbehörden der Länder eigene MUSS-Listen, so zum Beispiel in Thüringen:

https://tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf

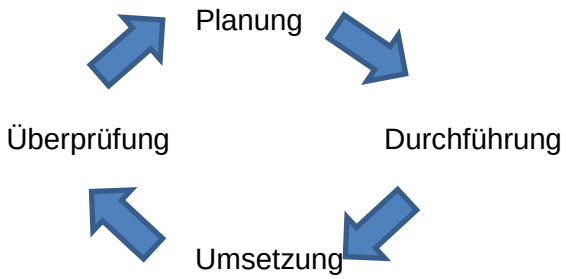
Die Mitgliedsunternehmen sind also gut beraten, sich auch zu erkunden, ob in ihrem jeweiligen Bundesland eine eigene MUSS-Liste besteht, da diese im Zweifel für die Beurteilung durch die jeweilige Aufsichtsbehörde maßgeblich ist.

Fazit: Im Zweifel ist den Unternehmen zu empfehlen, eine DSFA vorzunehmen!

3. Empfehlungen zum Vorgehen Datenschutz

Wenn eine Datenverarbeitung geplant ist, für die nach der MUSS-Liste oder im Zweifel eine DSFA erfolgen muss, so sollte das Unternehmen am besten wie folgt entsprechend der Empfehlungen der Aufsichtsbehörden vorgehen, um die Datenverarbeitung rechtmäßig vornehmen zu können.

Danach empfiehlt sich nach dem sog. Standard-Datenschutz-Modell (SDM) ein ständiger Kreislauf aus



In der Planungs- und Vorbereitungsphase der Datenverarbeitung und der parallelen DSFA werden zunächst die verantwortlichen Mitarbeiter benannt, die berührten Abteilungen erfasst und der Umfang der Datenverarbeitung geprüft und festgelegt. Dann erfolgt eine Bewertung der Notwendigkeit und der Verhältnismäßigkeit der Datenverarbeitung im Hinblick auf den gewünschten Zweck sowie die Prüfung der Rechtsgrundlagen.

In der Durchführungsphase werden dann zunächst alle Risiken, die den Schutz und die Freiheit der personenbezogenen Daten gefährden könnten, erfasst und beurteilt, um auf dieser Basis die geeigneten Schutz- und Abhilfemaßnahmen gegen diese Risiken zu definieren und in einem DSFA Bericht festzuhalten. Der DSFA - Bericht beinhalte jedenfalls

- die systematische Beschreibung der geplanten Verarbeitungs-vorgänge und ihrer Zwecke,
- die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung,
- die Beschreibung und Beurteilung der Risiken sowie
- die Beschreibung der Abhilfemaßnahmen zur Risikoeindämmung.

Achtung! Bußgeld-Gefahr:

Ergibt eine Risikoabwägung im Rahmen der DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht („Restrisiko“), muss das Unternehmen nach Art. 36 DSGVO die zuständige Aufsichtsbehörde konsultieren.

In der Umsetzungsphase werden die zuvor definierten Schutz- und Abhilfemaßnahmen implementiert, getestet und dokumentiert. Erst wenn dies erfolgt ist, darf mit der Verarbeitung begonnen werden.

In regelmäßigen Abständen und bei jeder wesentlichen Änderung der Datenverarbeitung ist die DSFA in der Überprüfungsphase auf Ihre Wirksamkeit und Rechtmäßigkeit zu überprüfen. Ergibt sich aus der Überprüfung ein Handlungsbedarf, so ist dieser mit der Planungsphase beginnend wieder im Zyklus der SDM abzuarbeiten.

4. Empfehlungen des Ausschusses Datenschutz

Der DRV-Ausschuss Datenschutz empfiehlt den Mitgliedsunternehmen grundsätzlich, umfangreiche Datenverarbeitungen, die über die Abwicklung einer einzelnen konkreten Reisebuchung und der Betreuung der Reisenden im Rahmen dieser Reisebuchung hinausgehen, im Hinblick auf eine möglicherweise notwendige DSFA zu überprüfen.

Auch wenn die Vorprüfung ergeben sollte, dass keine DSFA notwendig ist, empfiehlt es sich, dieses Ergebnis durch das Datenschutzteam zu dokumentieren.

5. Weiterführende Hinweise

Kurzpapier der DSK zur DSFA:

https://www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf

Themenschwerpunkt des BayLDA zur DSFA:

https://www.lda.bayern.de/de/dsfa.html

Ausführliche Dokumentation eines Beispiels („Planspiel“) der Aufsichtsbehörden zur DSFA beim ULD Schleswig-Holstein:

https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf

Disclaimer:

Unsere Datenschutzhinweise werden auf der Grundlage der uns bekannten Rechtsprechung und Literatur erstellt. Es gibt noch keine Erfahrungswerte mit der Auslegung zum neuen Datenschutzrecht. Wir können nicht ausschließen, dass ein Gericht zu einer anderen Bewertung kommt. Wir bitten daher um Verständnis, dass wir insofern keine Haftung übernehmen können.