Muster mit Hinweisen für die Durchführung

einer Risiko- und Datenschutzfolgenabschätzung (DSFA)

nach § 67 BDSG (Stand 10.02.2020)[1)]

A. Bezeichnung der Verarbeitung

1. Name der Verarbeitung: ☐
2. Standort im Verfahrensverzeichnis *(laufende Nr. o.ä.)*: ☐
3. Verantwortliche Arbeitseinheit *(interne Verantwortlichkeit)*: ☐
4. Besteht eine Errichtungsanordnung?

   ☐ Ja [2)]

   ☐ Nein

B. Beschreibung der Verarbeitung

1. Werden bei der Verarbeitung neue Technologien *(z.B. neue Datenmodelle)* verwendet?

   ☐ Ja Falls ja, Begründung:

   ☐ Nein ☐

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

2. Art der Verarbeitung *(z.B. Bewertung, Prognose, Profiling, automatisierte Entscheidung nach § 54 BDSG)*:

3. Umfang der Verarbeitung *(z.B. Datenmenge, geographisches Ausmaß, Beschränkung auf bestimmte Phänomene / Delikte, Anteil der erfassten Personen an der betroffenen Bevölkerungsgruppe)*:

4. Umstände der Verarbeitung *(z.B. Eingriffsintensität der zur Datenerhebung eingesetzten Mittel, verdeckte Datenerhebung, Benachrichtigung der Betroffenen, Verfahrenssicherungen wie Richtervorbehalte oder Einwilligungserfordernisse, Eingriffsintensität der mit der Verarbeitung bezweckten Maßnahmen (z.B. Ausreisebeschränkung), Fernzugriff durch Telearbeit / mobiles Arbeiten, dezentrale oder zentrale Datenhaltung, Sortierbarkeit, Verknüpfungsmöglichkeiten)*:

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

5. Zwecke der Verarbeitung:

☐ Aufgabenerfüllung

☐ Dokumentation

☐ Vorgangsverwaltung

☐ Gefahrenabwehr

☐ Strafverfolgung

☐ Strafverfolgungsvorsorge

Erläuterung:

6. Beschreibung des Personenkreises, dessen Daten verarbeitet werden:

Werden Daten von Personen verarbeitet, die keinen Anlass für ihre Speicherung gegeben haben?

☐ Ja

☐ Nein

Falls ja, Begründung:

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Werden Daten von Personen verarbeitet, für deren Speicherung eine Negativprognose erforderlich ist?

☐ Ja Falls ja, Begründung:

☐ Nein

Werden Daten von besonders schutzbedürftigen Personen verarbeitet *(z.B. Kinder, Asylbewerber, Opfer)*?

☐ Ja Welche?

☐ Nein

7. Beschreibung der Datenarten, die verarbeitet werden *(z.B. Name, Geburtsdatum)*:[3)]

Werden auch persönliche Einschätzungen im Sinne des § 73 BDSG verarbeitet?

☐ Ja Falls ja, Begründung:

☐ Nein

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Werden besondere Kategorien personenbezogener Daten nach § 46 Nr. 14 BDSG verarbeitet?

☐ Ja Falls ja, Begründung:

☐ Nein

8. Beschreibung der vorgesehenen Kennzeichnungen *(z.B. Zweckbindung, Sortierkennzeichen für Deliktsgruppen/ Phänomenbezüge etc., Eingriffsintensität, StPO-Kennzeichnungen, Zugriffsberechtigungen, Speicherdauer, Aussonderungsprüffristen)*:

9. Beschreibung der Rechtsgrundlagen für die Verarbeitung:

10. Beschreibung der betroffenen Rechte und Freiheiten der betroffenen Personen:

11. Angaben zu Abrufberechtigungen und Übermittlungsempfängern:

    a. Interne Zugriffsberechtigungen:

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

b. Externe Abrufberechtigungen (z.B. automatisierte Abrufe):

c. Eingerichtete Schnittstellen:

d. Übermittlungsempfänger:

12. Speicherdauer und Aussonderungsprüffristen:

13. Protokollierung nach § 76 BDSG oder Fachrecht
(insbesondere Speicherort und zuständige Organisationseinheit, Analysefähigkeit, Zugriffsberechtigungen, sonstige Maßnahmen zur Sicherstellung der Zweckbindung):

C. Risikoabschätzung

(immer durchzuführen)
Hat die Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr[4)] für die Rechtsgüter[5)] der betroffenen Personen zur Folge?

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

1. Liegt ein Verarbeitungsvorgang vor, der in der durch den BfDI erstellten Liste nach § 69 Abs. 1 S. 2 BDSG („Blacklist“) aufgeführt ist? *(Hinweis: Eine solche Liste wird derzeit nicht geführt.)*

   ☐ Ja — Folge: Durchführung einer DSFA ist immer erforderlich.

   ☐ Nein

2. Hat die Verarbeitung aufgrund ihrer Art (siehe oben unter B.2.) voraussichtlich eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge?

   ☐ Ja — Falls ja, Begründung:

   ☐ Nein

3. Hat die Verarbeitung aufgrund ihres Umfangs (siehe oben unter B.3.) voraussichtlich eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge?

   ☐ Ja — Falls ja, Begründung:

   ☐ Nein

4. Hat die Verarbeitung aufgrund ihrer Umstände (siehe oben unter B.4.) voraussichtlich eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge?

   ☐ Ja — Falls ja, Begründung:

   ☐ Nein

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

5. Hat die Verarbeitung aufgrund ihrer Zwecke (siehe oben unter B.5.) voraussichtlich eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge?

☐ Ja Falls ja, Begründung:

☐ Nein

6. Ergibt sich aus einer Gesamtbetrachtung von Art, Umfang, Umständen und Zwecken der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen?

☐ Ja Falls ja, Begründung:

☐ Nein

Zwischenergebnis:

☐ Es liegt ein Fall des § 69 Abs. 1 S. 2 BDSG („Blacklist“) vor (s.o. unter C.1.).

⇨ Weiter mit D.

☐ Es liegt eine erhebliche Gefahr vor.
(oben unter C.2-6. wurde mindestens einmal „ja“ angekreuzt)

⇨ Weiter mit D.

☐ Es liegt kein Fall des § 69 Abs. 1 S. 2 BDSG („Blacklist“) vor (s.o. unter C.1.) und es liegt keine erhebliche Gefahr vor *(oben unter C.2.-6. wurde nur „nein“ angekreuzt)*.

⇨ Beteiligung des bDSB

⇨ Sicherstellung der Dokumentation

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

D. Datenschutzfolgenabschätzung

1. Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Art, Umstände, Umfang und Zweck[6)]

   a. Was ist der legitime Zweck der Verarbeitung?

   b. Sind Art, Umstände und Umfang der Verarbeitung zur Erreichung dieses Zweckes geeignet? Warum?

   c. Sind Art, Umstände und Umfang der Verarbeitung zur Erreichung dieses Zweckes erforderlich? Warum?

   d. Gibt es mildere Mittel zur Erreichung desselben Zweckes? Wenn ja, welche? Warum sind diese nicht in gleicher Weise zur Erreichung des Zweckes geeignet?

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

e. Steht die Verarbeitung nach Art, Umständen und Umfang und der daraus resultierenden Schwere des Eingriffs in die Rechte und Freiheiten der betroffenen Personen nicht außer Verhältnis zum Zweck? Ist der Eingriff zumutbar?

2. Identifikation und Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen[7)]

   Hier ist eine methodische Bewertung der ermittelten Risiken vorzunehmen. Ein Vorschlag zum Vorgehen befindet sich in der Anlage.

3. Ermittlung und Dokumentation der technischen und organisatorischen Maßnahmen zur Bewältigung der identifizierten Risiken / zur Gewährleistung eines angemessenen Schutzniveaus (§ 64 BDSG)[9)]:

   a. Welche Maßnahmen sind / werden umgesetzt?

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

b. Wird / wurde die Wirksamkeit überprüft?

4. Wurde geprüft, ob die technischen und organisatorischen Maßnahmen alle identifizierten Risiken abdecken?

Zwischenergebnis:

☐ Es liegt ein Fall des § 69 Abs. 1 S. 2 BDSG („Blacklist“) vor (s.o. unter C.1.).

⇨ Anhörung des BfDI ist durchzuführen.

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

☐ Die Verarbeitung hat - trotz der getroffenen Schutzmaßnahmen - eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge, § 69 Abs. 1 S. 1 Nr. 1 BDSG.

Begründung:

⇨ Anhörung des BfDI ist durchzuführen.

☐ Durch die getroffenen Schutzmaßnahmen werden die oben festgestellten Risiken für die Rechte und Freiheiten der betroffenen Personen minimiert oder abgewehrt

⇨ Beteiligung des bDSB

⇨ Sicherstellung der Dokumentation

☐ Die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, hat eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge, § 69 Abs. 1 S. 1 Nr. 2 BDSG.

⇨ Anhörung des BfDI ist durchzuführen.

E. Anhörungsverfahren

Übersendung der Unterlagen nach § 69 Abs. 2 BDSG am: | |

Stellungnahme BfDI eingegangen am: | |

Ergebnis: | |

F. Abschluss der DSFA

⇨ Beteiligung bDSB

⇨ Sicherstellung der Dokumentation

⇨ Überprüfung der DSFA bei Änderungen an der Datenverarbeitung, Datenschutzverletzungen sowie in regelmäßigen Abständen

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Hinweise:

1) Dieses Muster bildet den aktuellen Stand in einem laufenden Entwicklungsprozess ab und soll bei Bedarf anhand von Erkenntnissen aus der künftigen Praxis, Impulsen aus der datenschutzrechtlichen Literatur und Vorgaben der Rechtsprechung fortentwickelt werden.

   Die DSFA soll als Hilfestellung dafür dienen, Risiken der Datenverarbeitung rechtzeitig zu erkennen. Sie soll formalisiert eine Hilfestellung leisten, etwa bei Ermessensentscheidungen den Umfang der noch verhältnismäßigen Datenverarbeitung bestimmen zu können oder auf Tatbestandsebene erkennen zu können, ob eine Datenverarbeitung noch erforderlich ist (z.B. fraglich bei fehlender Datenminimierung). Ferner kann sie etwa zu beurteilen helfen, ob die allgemeinen Vorgaben des § 47 BDSG beachtet sind. Sie entbindet aber nicht von der rechtlichen Prüfung der Voraussetzungen der Datenverarbeitung, die getrennt davon durchzuführen und nicht durch das Ergebnis der DSFA präjudiziert ist. Aus praktischen Gründen sollten die rechtlichen Voraussetzungen in der Dokumentation aber dargestellt werden, da sonst die geplante Verarbeitung nicht bestimmbar ist. Zudem sind die Details der Datenverarbeitung in die DSFA-Dokumentation aufzunehmen, weil sonst auch die Risikoabschätzung nicht möglich ist.

   Die DSFA und das Verfahrensverzeichnis sind organisatorische und verfahrensrechtliche Vorkehrungen, welche der Datenschutzaufsichtsbehörde ihre Kontrolle ermöglichen bzw. unterstützen sollen. Diese sind auch deshalb besonders bedeutsam, weil sonst die verantwortliche Stelle ein erhebliches rechtliches Risiko eingeht. Liegen die Dokumente nicht vor, könnte dies dazu führen, dass die Behörde die Daten formell rechtswidrig verarbeitet. Dies verletzt die subjektiven Rechte der betroffenen Person. Diese kann sich darauf bei Gericht berufen, eine Klage wäre dann formell zulässig und materiell begründet (vgl. OVG Lüneburg, Urteil vom 18. Oktober 2019 – 11 LC 148/15 –, juris, Rn. 74).

   Die DSFA ist ein eigenes Instrument zur Risikoabschätzung. Sie ersetzt nicht die Dokumentation des Verfahrens. Insoweit muss die Verarbeitung in ihren Einzelheiten auch aus dem Verfahrensverzeichnis ersichtlich sein.

2) Soweit für die betreffende Verarbeitung auch eine Errichtungsanordnung (EAO) zu erstellen ist, kann in der Beschreibung der Verarbeitung unter Teil B darauf verwiesen werden. Allerdings sollte dies nicht pauschal, sondern jeweils zu den

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

einzelnen Unterpunkten auf spezifische Ziffern in der EAO erfolgen, um sicherzustellen, dass alle erforderlichen Angaben abgedeckt sind.

3) Bei der Darstellung der in der Verarbeitungstätigkeit enthaltenen Daten sollte nicht pauschal auf die Daten nach einer ggf. einschlägigen Rechtsverordnung verwiesen werden, deren Verarbeitung grundsätzlich zulässig ist. Es kommt darauf an, welche Daten in der bestimmten Verarbeitung konkret verarbeitet werden. Sind dies im konkreten Fall alle nach einer Rechtsverordnung zugelassenen Daten, ist dies ausdrücklich festzuhalten.

4) Der in § 67 BDSG verwendete Begriff der „Gefahr“ ist nicht im Sinne des deutschen Polizei- und Ordnungsrechts auszulegen, sondern mit Blick auf die europarechtliche Vorgabe der JI-Richtlinie und den dort in Art. 27 Abs. 1 ebenfalls verwendeten Begriff des „hohen Risikos“ (vgl. dazu auch Hansen in: Wolff/Brink, BeckOK Datenschutzrecht, 24. Edition, § 67 BDSG Rn. 8). Trotz des unterschiedlichen Wortlautes besteht somit kein inhaltlicher Unterschied zwischen dem „hohen Risiko“ nach der DSGVO und der „erheblichen Gefahr“ nach § 67 BDSG.

5) Unter „Rechtsgüter“ im Sinne des § 67 BDSG sind sämtliche Rechte und Freiheiten der betroffenen Person gemeint (vgl. Erwägungsgrund 51 der JI-Richtlinie).

6) Bei der nach § 67 Abs. 4 BDSG gebotenen Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck ist auf die Eignung, Erforderlichkeit und Verhältnismäßigkeit der konkreten Ausgestaltung abzustellen. Soweit der Gesetzgeber die Datenverarbeitung als solche bereits für gesetzlich zulässig erklärt hat, muss dieses in der DSFA nicht als Teil der Abwägung dargestellt werden. Die Abwägung muss sich vielmehr mit dem vom Gesetzgeber verfolgten Einzelziel auseinandersetzen. Soweit der Gesetzgeber der verantwortlichen Stelle Spielraum eingeräumt hat, sind die Ziele der Datenverarbeitung im Einzelnen darzustellen.

7) Die Identifikation und Bewertung der Risiken bildet den Kern der DSFA.

   An dieser Stelle ist deutlich zwischen den Gewährleistungszielen des Datenschutzes und der IT-Sicherheit zu unterscheiden. Zwar verfolgen Datenschutz und IT-Sicherheit zum Teil gleichlautende Gewährleistungsziele. Im Bereich der IT-Sicherheit werden diese jedoch aus Sicht des Verantwortlichen und dessen Interessen verfolgt, im Datenschutz aus der Perspektive der Grundrechtsträger (zur Erläuterung des Zusammenspiels vgl. auch Standarddatenschutzmodell der DSK, Version 2.0, November 2019, S. 57). Viele technisch-organisatorische Maßnahmen

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

kommen sowohl dem Datenschutz als auch der IT-Sicherheit zugute, und entsprechende Synergie-Effekte sind durchaus anzustreben. Die Bewertung der datenschutzrechtlichen Risiken ist jedoch nach eigenständigen Maßstäben und unabhängig von der Bewertung der IT-Sicherheitsrisiken durchzuführen. Hier sollte kein innerer Zusammenhang hergestellt werden.

Darüber hinaus erscheint es empfehlenswert, den Risikobewertungsprozess in einer strukturierten Form nach einer vorgegebenen Systematik durchzuführen, um die Wahrscheinlichkeit zu erhöhen, dass Risiken der Datenverarbeitung rechtzeitig erkannt werden.

Im bereits zitierten Standarddatenschutzmodell (SDM) und im DSK-Kurzpapier Nr. 18, die weitgehend auf den JI-Bereich übertragbar sind, werden für diesen Prozess jeweils drei Leitfragen aufgestellt, die zur Orientierung dienen können:

- Welche Schäden können für betroffene Personen auf der Grundlage der zu verarbeitenden Daten auftreten?
- Wodurch d.h. durch welche Ereignisse kann es zu dem Schaden kommen?
- Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?

Um orientiert an diesen Leitfragen potentielle Schadensereignisse systematisch und nach Möglichkeit lückenlos zu bestimmen, sind verschiedene Methoden denkbar. Die beigefügte Anlage schlägt als Methode vor, die einzelnen Gewährleistungsziele des Datenschutzes jeweils in Kombination mit typischen Risikoquellen auf potentielle Schadensereignisse zu untersuchen.

Als Gewährleistungsziele werden hierbei folgende zugrunde gelegt: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit (vgl. SDM, Teil A. 4).

Als Risikoquellen werden hierbei folgende zugrunde gelegt: die wie geplant durchgeführte Verarbeitung, die fehlerhafte Verarbeitung, die vorsätzlich missbräuchliche Verarbeitung (Mitarbeiterexzess), die fehlerhafte Verarbeitung bei Empfängern, technische Fehler, Angriffe von außen und höhere Gewalt / Naturkatastrophen (vgl. DSK Kurzpapier Nr. 18, Ziff. IV.1.b).

Für die identifizierten möglichen Schadensereignisse sind sodann jeweils Eintrittswahrscheinlichkeit und Schadensausmaß zu bestimmen. Die bereits

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

implementierten / vorgesehenen TOM sind hierbei zu berücksichtigen. Aus der Kombination beider Parameter ergibt sich sodann die Risikoeinstufung z.B. innerhalb einer Risikomatrix (vgl. DSK-Kurzpapier Nr. 19, Ziff. IV.3).

Diese Methode dient nur als Hilfestellung, Risiken für den Datenschutz und für die technische Sicherheit besser erkennen zu können. Dies kann etwa dazu dienen, die gesetzlichen Vorgaben des § 47 BDSG für die geplante Datenverarbeitung konkretisieren und einhalten zu können. Sie entbindet natürlich nicht von der materiellen Prüfung, ob die geplante Datenverarbeitung nach den geltenden gesetzlichen Bestimmungen zulässig ist. Vielmehr soll sie dabei unterstützen.

8) Beim potentiellen Schadensausmaß sind alle denkbaren negativen Folgen zu betrachten u.a. Diskriminierung, Identitätsdiebstahl oder -betrug, finanzieller Verlust, Rufschädigung, wirtschaftliche / gesellschaftliche Nachteile, erschwerte Rechtsausübung o. Kontrolle, Ausschluss / Einschränkung der Ausübung von Rechten und Freiheiten („chilling effect“), Profiling, körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter o. offengelegter Daten. Zu berücksichtigen ist sowohl die Intensität der Beeinträchtigung (z.B. Streubreite, Heimlichkeit) als auch die besondere Empfindlichkeit (z.B. sensitive Daten, Berufsgeheimnisträger, besonders geschützte Grundrechte und Rechtspositionen).

9) Bei der Darstellung der Schutzmaßnahmen ist an dieser Stelle insbesondere darzustellen, ob und welcher Mehrbedarf an TOM für die konkrete Verarbeitung gegenüber dem allgemeinen Sicherheitsniveau besteht und wie dieser umgesetzt wird.

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de