Checkliste: Die Datenschutz-Folgenabschätzung (DSFA) nach der EU-DS-GVO (Stand 26.10.2017; siehe auch Wybitul, EU-Datenschutz-Grundverordnung im Unternehmen, Praxisleitfaden, 1. Auflage, 2016, 41-43).

# 1. Vorbereitungsphase: Strukturen und Prozesse für DSFA einführen

* Ist die Umstellung auf die DS-GVO in der Organisation als Projekt organisiert, in dem die Interessenvertretung von Beginn an in das Projektteam einbezogen ist?
* Werden Änderungen im nationalen Datenschutzrecht kontinuierlich verfolgt, u.a. das Ausführungsgesetz zur DS-GVO, das zu einem neuen BDSG geführt hat?
* Liegt eine Übersicht in der Organisation vor, zu welchen Datenverarbeitungen, IuK-Systemen und Überwachungssystemen am Arbeitsplatz bereits Vorabkontrollen nach § 4d Abs. 5 und 6 BDSG a.F. durchgeführt worden sind?
* Liegen für die bisherige *interne Vorabkontrolle* Mustervorlagen und Standards vor, die ggf. an die neuen Vorgaben der DS-GVO für die DSFA angepasst werden können?
* Ist für Implementierung der DSFA ein unabhängiges Team benannt worden, das weisungsfrei arbeiten kann und vom Verantwortlichen mit den erforderlichen Ressourcen unterstützt wird?
* Sind beteiligte Akteure, Strukturen und Prozesse für eine *grundrechtskonforme* Datenschutz-Folgenabschätzung (DSFA) vorab festgelegt und mit der Interessenvertretung beraten worden?
* Sind alle Akteure einer DSFA über den Umgang mit Geschäfts- und Betriebsgeheimnissen bei der Erstellung einer DSFA geschult?
* Wird für jeden Fall einer DSFA oder der Prüfung der Erforderlichkeit einer DSFA der Rat des betrieblichen bzw. behördlichen Datenschutzbeauftragten nach Art. 35 Abs. 2 DS-GVO eingeholt, seine/ihre Stellungnahme und mögliche Abweichungen vom eingeholten Rat dokumentiert (Nachweispflicht)?
* Rechtspraxis: Muss der Datenschutzbeauftragte entgegen der DS-GVO in der Praxis die DSFA selbst erstellen und regelmäßig den Aktualisierungsbedarf überprüfen?
* Ist schriftlich festgelegt, dass die *oberste Leitung* für die Beurteilung von Verarbeitungen in einer DSFA verantwortlich ist?
* Sind innerbetrieblich die Kriterien einschließlich Indizien für die Erforderlichkeit einer DSFA bei Verarbeitungen festgelegt und mit dem Datenschutzbeauftragten, ggf. der Aufsichtsbehörde und der Interessenvertretung abgestimmt?
* Ist die Positivliste, die die Aufsichtsbehörden für die Erforderlichkeit einer DSFA erstellen, soweit vorliegend, bekannt und werden sie fortlaufend abgerufen?
* Sind die *maßgeblichen Rechtsgrundlagen* für die geplanten Datenverarbeitungen identifiziert und den Zwecken der Datenverarbeitung zugeordnet?
* Sind die in der DS-GVO genannten Schutzziele Datensparsamkeit, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit (Eingreifbarkeit) angemessen operationalisiert beschrieben?
* Sind vordefinierte Kataloge für Gewährleistungsziele nach Art. 5 Abs.1 DS-GVO, Bewertungskriterien, berechtigte Interessen und typische Schutzmaßnahmen für die Informationssicherheit erstellt worden, mit denen die konkreten Verarbeitungsvorgänge intern und extern in einem Soll-Ist-Vergleich geprüft werden können?
* Existiert eine schriftliche Anleitung zur Ermittlung der Erforderlichkeit (Art. 5 Abs. 1 lit. c DS-GVO) und des Schutzbedarfs der Daten?
* Ist festgelegt, in welchen Abständen und bei welchen Anlässen, ggf. auch von einer unabhängigen Stelle, überprüft werden soll, ob die Datenverarbeitung in der Praxis gemäß der dokumentierten DSFA durchgeführt wird und ob die DFSA fortzuschreiben ist?
* Wird das Standardmodell der Datenschutzkonferenz vom 9. und 10.11.2016 (Aufsichtsbehörden) in der Version 1.0 als Blaupause für die DSFA genutzt? Mehr unter <https://www.datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf>

# 2. Durchführungsphase: Inhalte, Bewertung, Maßnahmen, Dokumentation/Bericht bei einer DSFA

* Liegt für die Erstellung einer DSFA und zur Schaffung von Transparenz einer geplanten Verarbeitung (Prüfgegenstand) stets eine systematische Dokumentation der geplanten Verarbeitungsvorgänge, der Zwecke, der besonderen Datenkategorien und der berechtigten Interessen des Verantwortlichen vor?
* Liegt das Verzeichnis von Verarbeitungsaktivitäten nach Art. 30 Abs. 1 DS-GVO als Grundlage für die aktuell zu erstellende DSFA vor?
* Sollen personenbezogene Daten der Beschäftigten an wen und zu welchem Zweck weitergegeben oder in Drittstaaten übermittelt werden?
* Wird geprüft, wer Zugriff auf die personenbezogenen Daten hat und welche Aufbewahrungs- bzw. Löschfristen geplant bzw. einzuhalten sind?
* Sind die Zwecke des Prüfobjektes (Daten, Systeme, Prozesse) abschließend definiert und werden die Grundsätze der DS-GVO nach Art. 5 Abs. 1 wie z.B. Zweckbindung und Datenminimierung eingehalten?
* Werden die konkreten Risiken, die Motive und mögliche Verursacher für Angriffe für den speziellen Fall der DSFA ermittelt und bewertet?
* Sind für die *Nachweispflicht* nach Art. 5 Abs. 2 DS-GVO klare Vorgaben für die Dokumentation der Ergebnisse der durchgeführten DSFA und für auch den Fall getroffen worden, dass ggf. keine DSFA durchgeführt wird?
* Wird der abschließende *DSFA-Bericht* ganz oder ggf. in einer Kurzfassung veröffentlicht?
* Wird die Wirksamkeit der umgesetzten Abhilfemaßnahmen zur Eindämmung der konkreten Risiken angemessen getestet, kontrolliert und dokumentiert?
* Wird die DSFA stets **vor Inbetriebnahme** einer geplanten Datenverarbeitung durchgeführt?

# 3. Interessenvertretungen und die DSFA

* Liegt eine interne betriebliche Richtlinie mit einem Ablaufschaubild zur DSFA vor?
* Einbeziehung Betroffener und ihrer Vertreter: Hat der Verantwortliche bei der DSFA für Transparenz gesorgt, indem er nach Art. 35 Abs. 9 DS-GVO den Standpunkt der Beschäftigten oder ihrer Vertreter (z. B. Betriebs- und Personalräte, Gewerkschaften, Verbraucherschutzverbände) eingeholt hat bzw. vor allem die Vertreter umfassend konsultiert hat, ob eine DSFA durchgeführt werden muss und auch im Rahmen der Durchführung einer DSFA?
* Hat der Verantwortliche bzw. Auftragsverarbeiter sich zumindest mit den Standpunkten der Interessenvertretungen und Beschäftigten auseinandergesetzt und ist darauf in der Folgenabschätzung eingegangen?
* Wird der Betriebs- oder Personalrat dabei rechtzeitig und umfassend über Daten, Systeme und Prozesse im Rahmen der geplanten Datenverarbeitung informiert?
* Sind die betroffenen Beschäftigten über die geplante Datenverarbeitung im Sinne der DS-GVO informiert worden bzw. sind die Informationspflichten des Verantwortlichen erfüllt?
* Sind die Maßnahmen zur Datensicherheit nach Art. 32 DS-GVO als Sicherheitskonzept dokumentiert und ggf. mitbestimmt und liegen in jeder DSFA als Katalog technisch-organisatorischer Standardmaßnahmen vor?
* Hat der betriebliche Datenschutzbeauftragte seine Empfehlungen und Risikoabwägungen (Soll-Ist-Vergleich) und deren betriebliche Umsetzung bei den einzelnen einzuführenden Datenverarbeitungen bzw. sensiblen Verarbeitungsvorgängen dokumentiert und ggf. oder auf Anfrage als Unterlage der Interessenvertretung zur Verfügung gestellt?
* Lädt der Betriebsrat die DSFA-Akteure als interne Auskunftspersonen regelmäßig in die Sitzungen des Gremiums oder IT-Ausschusses ein?
* Erhält die Interessenvertretung vor Verhandlungen mit dem Arbeitgeber zu einzelnen Überwachungssystemen den DSFA-Bericht vom Verantwortlichen ausgehändigt?
* Geht die Interessenvertretung davon aus, dass bei Überwachungssystemen am Arbeitsplatz auf jeden Fall eine DSFA durchgeführt werden muss?

# 4. Art. 35 DS-GVO

**[EU-DSGVO] Datenschutz-Grundverordnung; [Verkündungsblatt ausgewertet bis 29.12.2016]; Art. 35: Zukünftige Fassung - Text gilt ab 25.05.2018**

**Artikel 35 Datenschutz-Folgenabschätzung**

(1) 1Hat eine 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, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. 2Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den  
 Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen  
erforderlich:

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.

(4) 1Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1   
 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) 1Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. 2Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a)eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Geltungszeitraum: ab 25.05.2018

# 5. BDSG-Neu (Entwurf): Bestimmungen zur DSFA

Stand: 2. Ressortabstimmung (11.11.2016, 16:13); Referentenentwurf des Bundesministeriums des Innern Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

**§ 61 Durchführung einer Datenschutzfolgenabschätzung**

[Art. 27 DS-RL] (1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine hohe Gefährdung für die Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.

(2) [Art. 35 Abs. 1 Nr. 2 DS-GVO] Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefährdungspotential kann eine einzige Abschätzung vorgenommen werden.

(3) [Art. 35 Abs. 2 DS-GVO] Der Verantwortliche beteiligt die Datenschutzbeauftragte oder den Datenschutzbeauftragten an der Durchführung einer Datenschutzfolgenabschätzung.

(4) [Art. 27 Abs. 2 DS-RL; Art. 35 Abs. 7 DS-GVO] Die Folgenabschätzung gemäß Absatz 1 trägt den Rechten der von der Verarbeitung betroffenen Personen und sonstiger betroffener Personen Rechnung und enthält zumindest Folgendes:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,

2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,

3. eine Bewertung der Gefährdung für die Rechtsgüter der betroffenen Person und

4. die zur Bewältigung der Gefahr geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die gesetzlichen Vorgaben eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger betroffener Personen Rechnung getragen wird.

(5) [Art. 35 Abs. 11 DS-GVO] Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben; dies gilt zumindest, wenn hinsichtlich der mit den Verarbeitungsvorgängen verbundenen Gefährdung Änderungen eingetreten sind.