



BGHP-Betriebsratsberater – Update Arbeitnehmerrecht (5/2018)

Was ist eine Datenschutz-Folgeabschätzung? Neugestaltung in der DSGVO

Ein Beitrag von Rechtsanwalt Martin Fieseler





Was ist eine Datenschutz-Folgeabschätzung?

Neugestaltung in der DSGVO

Die Datenschutz-Folgeabschätzung ist ein Instrument des Datenschutzes im Betrieb, das die Datenschutzgrundverordnung (DSGVO) zwar nicht ganz neu erfindet, aber wesentlich neu gestaltet:

Nach der bisher geltenden Rechtslage bedurfte jede automatisierte Verarbeitung, die besondere Risiken für die Rechte der Betroffenen aufwies, etwa weil Gesundheitsdaten verarbeitet wurden, grundsätzlich der Prüfung durch den betrieblichen Datenschutzbeauftragten auf ihre Rechtmäßigkeit ([§ 4d Abs. 5 und 6 BDSG](#)).

Diese Vorabkontrolle wird nun durch die Datenschutz-Folgeabschätzung ersetzt ([Art. 35 DSGVO](#)). Mit ihr werden risikoreiche Datenverarbeitungsvorgänge beschrieben und vor allem hinsichtlich der Risiken und Folgen für die Rechte der Betroffenen bewertet. Die DSGVO spricht dem Betriebsrat hierbei ein Beteiligungsrecht zu.

Woraus besteht die Datenschutz-Folgeabschätzung?

Die Datenschutz-Folgeabschätzung besteht aus folgenden Teilen:

- systematische Beschreibung der geplanten Verarbeitung und ihrer Zwecke
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der geplanten Verarbeitung
- Bewertung der Risiken für die Betroffenen
- Abhilfemaßnahmen zur Bewältigung der Risiken für die Betroffenen

(Bestandteile der Datenschutzfolgenabschätzung)

Bei den Abhilfemaßnahmen müssen auch die Vorkehrungen oder Verfahren dargestellt werden, die den Schutz personenbezogener Daten und die Einhaltung der Datenschutz-Grundverordnung sicherstellen.

Wer nimmt die Datenschutz-Folgeabschätzung vor?

Die Datenschutz-Folgeabschätzung führt nicht mehr der betriebliche Datenschutzbeauftragte, sondern der Arbeitgeber selbst durch. Dieser muss sich dabei jedoch vom betrieblichen Datenschutzbeauftragten beraten lassen (sofern ein solcher benannt ist). Die neue Rollenverteilung gibt dem Arbeitgeber zwar noch mehr



Verantwortung, hat aber den Nachteil, dass sie die Prüfung dem fachlich unabhängigen Datenschutzbeauftragten aus den Händen nimmt. Allerdings hat dieser die Durchführung der Datenschutz-Folgenabschätzung zu überwachen ([Art. 39 Abs. 1 c DSGVO](#)) und mit der Aufsichtsbehörde zusammenzuarbeiten.

Wann ist die Datenschutz-Folgenabschätzung durchzuführen?

Eine Datenschutz-Folgenabschätzung ist durchzuführen, wenn die Verarbeitungsform oder Art von Verarbeitungsvorgängen ein hohes Risiko für die Rechte der Betroffenen zur Folge hat ([Art. 35 DSGVO](#)). Dies kann der Fall sein, weil neue Technologien verwendet werden oder der Umfang oder Zweck der Verarbeitung risikoreich ist. Die DSGVO nennt als Beispiele, wann dies der Fall ist, die umfassende Bewertung persönlicher Aspekte (etwa der Leistung) Betroffener mit automatisierten Verfahren und die umfangreiche Verarbeitung von besonderen Daten – wie (weiterhin) Gesundheitsdaten. Diese Regelung ist im Vergleich zur bisherigen Rechtslage in Deutschland etwas großzügiger für die Daten verarbeitenden Arbeitgeber. Dies zeigt sich am Beispiel der Gesundheitsdaten:

Beispiel

*So reicht nicht mehr die Verarbeitung von Gesundheitsdaten überhaupt, damit eine Datenschutz-Folgenabschätzung nötig ist, sondern es müssen **umfangreich** Gesundheitsdaten verarbeitet werden. Bestehende Ausnahmen wurden dagegen abgeschafft.*

Eine Datenschutz-Folgenabschätzung ist in der Regel hinsichtlich der Verarbeitung von Beschäftigtendaten erforderlich, da es sich um eine risikoreiche Art oder Form der Verarbeitung handelt. Hierfür spricht das Wesen des Arbeitsverhältnisses:

- Es ist auf Dauer und Nähe angelegt.
- Es ist gekennzeichnet durch ein strukturelles Ungleichgewicht der Arbeitsvertragsparteien hinsichtlich betrieblicher Gestaltungsmacht und wirtschaftlicher Abhängigkeit.
- Besonders risikoreich ist die systematische und umfassende Bewertung persönlicher Aspekte, wie der Leistung von Beschäftigten in Personaldaten-Verarbeitungsprogrammen.



- Auch die Schutzwürdigkeit der verarbeiteten Daten, etwa der Gesundheitsdaten, oder die Zahl der erfassten Arbeitnehmer, sprechen für die Erforderlichkeit einer Datenschutz-Folgenabschätzung.

Welchem Zweck dient die Datenschutz-Folgenabschätzung?

Die Datenschutz-Folgenabschätzung dient dem **Ziel**, dass der für die Datenverarbeitung verantwortliche Arbeitgeber das Risiko von Datenverarbeitungsvorgängen einschätzt und sich bewusst macht.

Wichtig:

Die Datenschutz-Folgeabschätzung ist quasi die Gefährdungsbeurteilung des Datenschutzes

Bei hohen Risiken soll der Arbeitgeber

- transparent darstellen, welche Verarbeitung er vornimmt,
- hinterfragen, ob er die Verarbeitung wirklich für im Vorhinein bestimmte, legitime Zwecke benötigt
und
- prüfen, ob nicht doch die Interessen der Betroffenen überwiegen und welche Risiken für das Recht auf informationelle Selbstbestimmung der Mitarbeiter bestehen.

Weiter muss der Arbeitgeber mit der Datenschutz-Folgenabschätzung festlegen, welche **Abhilfemaßnahmen** er zur Bewältigung der Risiken implementiert. Dazu gehören zum Beispiel rechtlich bindende Garantien für die Mitarbeiter, technische Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird. Gleichzeitig soll der Arbeitgeber auf diese Weise nachweisen, dass er die DSGVO einhält, indem er dies schriftlich niederlegt und aufbewahrt.

Wann besteht eine Pflicht zur Konsultation der Aufsichtsbehörde?

Wenn die Datenschutz-Folgenabschätzung ein hohes Risiko für personenbezogene Daten ergibt, und der Arbeitgeber keine Maßnahmen zur Eindämmung des Risikos trifft, muss er vor der Verarbeitung die Aufsichtsbehörde konsultieren ([Art. 36 DSGVO](#)).

Diese Regelung stellt eine Einschränkung der Konsultationspflicht im Vergleich zur Rechtslage vor der DSGVO dar. Bisher bestand eine generelle Meldepflicht von



automatisierter Verarbeitungen personenbezogener Daten, wenn mehr als neun Beschäftigte mit der Verarbeitung betraut waren und kein betrieblicher Datenschutzbeauftragter bestellt war ([§ 4d Abs. 1 bis 4 BDSG](#)). Die Meldepflicht findet nun nicht mehr generell Anwendung, sondern nur noch, bei hohen Risiken, die nicht eingedämmt werden. Die DSGVO will, dass die Verantwortlichen ihre Aufmerksamkeit auf die risikobehafteten Verarbeitungsvorgänge richten. Dies wird als **risikobasierter Datenschutzansatz** bezeichnet.

Wenn die Aufsichtsbehörde um Konsultation ersucht wird, ist sie gehalten, dem Arbeitgeber schriftliche Empfehlungen zukommen zu lassen, wie er das Risiko eindämmen kann, sofern dies möglich ist. Notfalls kann die Aufsichtsbehörde die Verarbeitung verbieten oder anordnen, dass bereits verarbeitete Daten gelöscht werden.

Welche Beteiligungsrechte hat der Betriebsrat?

Hervorzuheben ist, dass die DSGVO den Arbeitgeber verpflichtet, den **Standpunkt** betroffener Personen oder, wenn es einen solchen gibt, des Betriebsrats zu der beabsichtigten Verarbeitung einzuholen ([Art. 35 Abs. 9 DSGVO](#)). Damit der Betriebsrat seinen Standpunkt darlegen kann, muss er vorher **unterrichtet** werden.

Die Konsultierung des Betriebsrats betrifft

- sowohl die Frage der Notwendigkeit der Datenschutz-Folgenabschätzung („**Ob**“) und damit das Vorliegen besonderer Risiken
- als auch die Durchführung der Folgenabschätzung selbst („**Wie**“).

Dies wird allgemein für Betroffenenvertreter auch in der Kommentarliteratur so gesehen (Paal/Pauly/Martini, DS-GVO Art. 35 Randnr. 60).

Mit seinem Standpunkt teilt der Betriebsrat dem Arbeitgeber mit, wie er

- die Verarbeitung,
- deren Notwendigkeit,
- deren Verhältnismäßigkeit und
- deren Risiken bewertet, sowie
- welche Maßnahmen er für erforderlich hält.



Der Verantwortliche muss sich mindestens mit dem Standpunkt auseinandersetzen und in der Datenschutz-Folgenabschätzung auf ihn eingehen.

Etwas komplett Neues regelt die Datenschutz-Grundverordnung hiermit – zumindest für das deutsche Recht – nicht, auch wenn das Beteiligungsrecht nach DSGVO und nach BetrVG in manchen Fällen auseinanderfallen können (z.B. Erfassung von Krankheiten). [§ 87 Abs. 1 Nr. 6 BetrVG](#) und [§ 80 Abs. 2 BetrVG](#) sehen schon bisher umfassende Beteiligungsrechte vor, die im Wesentlichen sogar noch weiter gehen, als die durch [Art. 35 Abs. 9 DSGVO](#) begründeten. Denn nach [§ 87 Abs. 1 Nr. 6 BetrVG](#) hat der Betriebsrat ein zwingendes Mitbestimmungsrecht, mit dem der Betriebsrat gleichberechtigt über die Einführung und Anwendung von technischen Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, mitbestimmen kann.

Praxistipp

Sofern noch nicht, beispielsweise in einer Rahmen-Betriebsvereinbarung geschehen, sollte der Betriebsrat mit dem Arbeitgeber ein Verfahren vereinbaren, wie sein Standpunkt zum Ob und Wie einer Datenschutz-Folgenabschätzung eingeholt wird bzw. sein Mitbestimmungsrecht umgesetzt wird. Dabei kommt der Vereinbarung einer Unterrichtung und Beteiligung rechtzeitig **vor** der Entscheidung über die Notwendigkeit der Folgenabschätzung und vor ihrer Durchführung entscheidende Bedeutung zu. Am besten ist es, einen genauen Zeitplan festzulegen. So werden mögliche Meinungsverschiedenheiten bereits im Vorfeld geklärt und stellt für beide Betriebsparteien eine gesetzesgemäße Beteiligung sicher.

Wo gibt es weitere Informationen zur Datenschutz-Folgenabschätzung?

Einen Überblick zur Datenschutz-Folgenabschätzung aus Sicht der Aufsichtsbehörden gibt deren [Kurzpapier Nr. 5 zur DSGVO](#). Ausführlicher hat die EU-Datenschutzgruppe in ihrem [Arbeitspapier WP 248](#) beschrieben, wie die Datenschutz-Folgenabschätzung funktionieren muss. Hervorzuheben ist in diesem Arbeitspapier die Checkliste im Anhang 2, die Kriterien für einen „Schnelltest“ enthält, ob die eigene Datenschutz-Folgenabschätzung umfassend genug ist, damit der DSGVO entspricht.



Wie die Datenschutz-Folgenabschätzung aussehen kann, so dass die Aufsichtsbehörden sie akzeptieren, zeigt das von ihnen erstellte [Standarddatenschutz-Modell](#).

Rechtsanwalt Martin Fieseler

Berger Groß Höhmann & Partner Rechtsanwälte

Danziger Straße 56

Telefon: 030-440 330-19

10435 Berlin / Prenzlauer Berg

Telefax: 030-440 330-22

E-Mail: fieseler@bg hp.de

www.bg hp.de

Die Autoren sind Rechtsanwälte der Berliner Kanzlei Berger Groß Höhmann & Partner. Wir vertreten im Arbeitsrecht ausschließlich Betriebsräte, Personalräte und Beschäftigte. Dabei legen wir Wert auf Individualität und den persönlichen, vertrauensvollen Kontakt. Unser Ziel ist es, lösungsorientiert gemeinsam mit unseren Betriebs- und Personalräten Strategien zu erarbeiten, um die Arbeitsbedingungen der Arbeitnehmer spürbar zu verbessern oder vor Verschlechterungen zu bewahren. Wir treten mit unserer Arbeit aktiv für einen sozialen, demokratischen Rechtsstaat ein, in dem Recht nicht nur das Recht des (Finanz-)Stärkeren ist. Unsere handlungsleitenden Grundsätze sind Solidarität, Stärkung von demokratischen (Teilhabe-)Rechten und wirtschaftlicher Mitbestimmung in Unternehmen.

Thomas Berger*	Fachanwalt für Arbeitsrecht
Dr. Johannes Groß M.A.*	Fachanwalt für Sozialrecht
Sebastian Höhmann*	Fachanwalt für Erbrecht
Thomas Ebinger, LL.M.*	Fachanwalt für Arbeitsrecht
Uwe Nawrot*	Fachanwalt für Arbeitsrecht
Karin Burth*	Fachanwältin für Arbeitsrecht
Katharina Behrens-v.Hobe	Fachanwältin für Sozialrecht
Stefanie Kirschner, LL.M.*	Fachanwältin für Arbeitsrecht
David-S. Schumann,	Rechtsanwalt, Dipl.-Ing. (FH)
Wolf Klimpe-Auerbach	Rechtsanwalt, Richter am Arbeitsgericht a. D.
Martin Fieseler	Rechtsanwalt (Arbeitsrecht)
Priyanthan Thilagaratnam	Rechtsanwalt (Arbeitsrecht)
Elisabeta Schidowezki	Rechtsanwältin (Erbrecht)
Stephan Puhlmann	Rechtsanwalt (Arbeitsrecht)



Betriebsratsberater

Ein Informationsservice von Berger Groß Höhmann & Partner

Christian Lunow	Rechtsanwalt (Arbeitsrecht)
Nele Kliemt	Rechtsanwältin (Erbrecht)
Dr. Katharina Wandscher	Rechtsanwältin (Arbeitsrecht)
Benedikt Rüdeshcim, LL.M.	Rechtsanwalt (Arbeitsrecht)
(*Partner)	

Unsere Beratungsseiten im Internet:

www.betriebsratsberater-berlin.de

www.pflegerechtsberater.de

www.erbrechtsberater-berlin.de

www.scheidungsrechtsberater.de