Law | GDPR:Obligations

O.15 Accountability Obligations

Authors: Winfried Veil

Last update: 2023-07-17 21:59:47 | By: Winfried Veil

Created at: 2021-05-27 21:46:41

[Translation coming soon]

Die DS-GVO enthält zahlreiche allgemeine und spezielle Nachweispflichten, die sich dem Grundsatz der Rechenschaftspflicht zuordnen lassen.

Generalklauselartig formuliert sind die folgenden Nachweispflichten des Verantwortlichen:

> ***Art. 5 II DS-GVO:*** *"*Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung **nachweisen** können." ? Der Verantwortliche muss also die Einhaltung der Grundsätze nachweisen können.

> ***Art. 24 I 1 DS-GVO:*** *"*Der Verantwortliche setzt [...] technische und organisatorische Maßnahmen um, um [...] den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt." ? Der Verantwortliche muss also seine Compliance mit der Verordnung nachwweisen können.

> ***EG 74 S. 2 DS-GVO:*** *"*Insbesondere sollte der Verantwortliche [...] **nachweisen** können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind." ? Der Verantwortliche muss also die Wirksamkeit seiner Maßnahmen nachweisen können.

Hinzu kommen die folgenden spezialgesetzlichen Nachweispflichten:

Einwilligung:

> ***Art. 7 I DS-GVO:*** *Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche die Einwilligung des Betroffenen **nachweisen** können (ebenso **EG 42 S. 1 DS-GVO**).*

Identitätsfeststellung:

Art. 11 II DS-GVO: *"*Kann der Verantwortliche [...] **nachweisen**, dass er nicht in der Lage ist, die betroffene Person zu identifizieren, [...] finden die Artikel 15 bis 20 keine Anwendung [...]*."*

Art. 12 II 2 DS-GVO: *"In den in Artikel 11 Absatz 2 genannten Fällen darf sich der Verantwortliche nur dann weigern, aufgrund des Antrags der betroffenen Person auf Wahrnehmung ihrer Rechte gemäß den Artikeln 15 bis 22 tätig zu werden, wenn er* ***glaubhaft macht****, dass er nicht in der Lage ist, die betroffene Person zu identifizieren.*

Art. 11 II und 12 II haben somit einen ähnlichen Inhalt. Wenn dem Verantwortlichen der Nachweis gelingt, dass er den Betroffenen nicht identifizieren kann, muss er bestimmte Betroffenenrechte nicht erfüllen. Allerdings bestehen zwischen den beiden Normen zwei Unterschiede:

- Während die englische Fassung in Art. 11 II und 12 II von „demonstrate“ spricht, verwendet die deutsche Fassung in Art. 11 II den Begriff „nachweisen“ und in Art. 12 II das schwächere „glaubhaft machen“.

- Während Art. 11 II auf die Art. 15 bis 20 verweist, verweist Art. 12 II auf die Art. 15 bis 22.

Widerspruch:

Art. 21 I 2: *"Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung* ***nachweisen*** *, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen [...]."*

EG 69 S. 2 *enthält in der englischen Fassung dieselbe Formulierung („demonstrate“). In der deutschen Fassung von EG 69 S. 2 wird „demonstrate“ allerdings mit dem gegenüber "nachweisen" schwächeren „darlegen“ übersetzt.*

Datenschutz „by design“ und „by default“:

Art. 25 I: *"[...] trifft der Verantwortliche [...] geeignete technische und organisatorische Maßnahmen [...], die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung* ***wirksam umzusetzen*** *[...]."*

Ergänzend heißt es in ***EG 78 S. 2:*** "Um die Einhaltung dieser Verordnung **nachweisen** zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun."

Dokumentation:

Art. 30: *Der Verantwortliche muss ein Verzeichnis aller Verarbeitungstätigkeiten führen, das dem Nachweis der Einhaltung der DS-GVO, wie sich aus* ***EG 82 S. 1*** *ergibt: "Zum* ***Nachweis*** *der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen."*

Das Verzeichnis muss unter anderem gemäß Art. 30 I e und II c bei Drittstaatenübermittlungen geeignete Garantien ***dokumentieren***.

Datensicherheit:

Art. 32: *Zur Gewährleistung der Sicherheit der Datenverarbeitung müssen der Verantwortliche und der Auftragsverarbeiter geeignete Maßnahmen treffen. Dazu gehören gemäß Art. 32 I d Verfahren zur regelmäßigen* ***Überprüfung***, ***Bewertung*** *und* ***Evaluierung*** *der Wirksamkeit der technischen und organisatorischen Maßnahmen. Um die Erfüllung der Anforderungen an die Datensicherheit* ***nachzuweisen***, *kommen Verhaltensregeln und Zertifizierungsverfahren als Faktoren in Betracht (Art. 32 III).*

Datenschutzverletzung:

Art. 33 V: *Der Verantwortliche muss Datenschutzverletzungen und die damit in Zusammenhang stehenden Fakten, Auswirkungen und Abhilfemaßnahmen* ***dokumentieren*** *. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen des Art. 33 ermöglichen. Nach* ***EG 85 S. 2*** *kann auf eine Notifikation bei der Aufsichtsbehörde verzichtet werden, wenn der Verantwortliche im Einklang mit dem Grundsatz der Rechenschaftspflicht* ***nachweisen*** *kann, dass die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Nach* ***EG 87 S. 1*** *sollte festgestellt werden, ob alle geeigneten Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Datenschutzverletzung aufgetreten ist, und um die Aufsichtsbehörde und den Betroffenen umgehend unterrichten zu können.*

Datenschutz-Folgenabschätzung:

Art. 35: *Die Datenschutz-Folgenabschätzung muss zumindest unter anderem die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren enthalten, durch die der Schutz personenbezogener Daten sichergestellt und der* ***Nachweis*** *dafür erbracht wird, dass diese Verordnung eingehalten wird (Art. 35 VII d). Nach* ***EG 84 Satz 2*** *sollen die Ergebnisse der Abschätzung bei der Entscheidung über die geeigneten Maßnahmen berücksichtigt werden, um* ***nachzuweisen***, *dass die Datenverarbeitung mit der DS-GVO in Einklang steht.*

Drittstaatentransfer:

> ***Art. 49:*** *In Fällen, in denen ein Drittstaatentransfer auf ein zwingendes berechtigtes Interesse des Verantwortlichen gestützt wird (Art. 49 I Unterabs. 2), muss der Verantwortliche alle Umstände der Datenübermittlung beurteilen und geeignete Garantien für den Schutz der Daten vorsehen. Beurteilung und Garantien müssen in der* ***Dokumentation*** *des Art. 30 erscheinen (Art. 49 VI).*

Haftung:

> ***Art. 82:*** *Der Verantwortliche oder der Auftragsverarbeiter werden von der Haftung für Schäden gemäß Art. 82 II befreit, wenn sie* ***nachweisen****, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich sind (Art. 82 III).*

Das EDPB leitet aus dem Grundsatz der Rechenschaftspflicht sogar noch weitere ungeschriebene Nachweispflichten ab (vgl. **WP 260 rev.01**). Auch das modifizierende deutsche Datenschutzrecht enthält weitere Nachweispflichten (z.B. §§ 22 II 2 Nr. 2, 25 II Nr. 2, 26 I 2 und II 3, 31 I Nr. 2 und Nr. 4, 32 II 2, 33 II 2, 34 II 1 BDSG).

Das Verhältnis der spezialgesetzlichen Nachweispflichten zu den allgemeinen Nachweispflichten der Art. 5 I und 24 I ist ungeklärt. Es spricht einiges dafür, dass die gesonderte Erwähnung einer Nachweispflicht in einer Einzelnorm im Rahmen der Risikoanalyse zu berücksichtigen ist. Ergibt die Risikoanalyse, dass ein Nachweis unter Risikogesichtspunkten gemäß Art. 24 nicht unbedingt erforderlich oder verhältnismäßig ist, kann sich aus der Einzelnorm unter Umständen doch eine Nachweispflicht ergeben, es sei denn, auch in der Einzelnorm steht die Nachweispflicht unter dem Vorbehalt der Risikoadäquanz. Enthält die Einzelnorm hingegen eine ausdrückliche Ausnahme von der Nachweispflicht, kann diese nicht über den Umweg von Art. 5 II und 24 I aufleben. Der Ausschluss der Nachweispflicht ist dann als *lex specialis* zur Regelung der allgemeinen Nachweispflicht anzusehen.

Umfang und Grenzen der Rechenschaftspflicht sind weitgehend unklar. Insbesondere ist unklar, welche Form die Nachweise haben müssen, welche zeitliche Grenze für die Aufbewahrung der Nachweise besteht, wie feingranular der Nachweis geführt werden muss und welche rechtlichen Folgen ein fehlender Nachweis hat. Bei sehr strengem Verständnis kann die Rechenschaftspflicht wohl nur durch umfassende Datenschutzmanagementsysteme erreicht werden. Zu weit gehende Nachweispflichten geraten aber in Konflikt mit den folgenden Rechtsgrundsätzen:

Impossibilium nulla est obligatio:

> *Es ist faktisch unmöglich, jedes einzelne Datum, jeden einzelnen Verarbeitungsschritt und jede einzelne technische und organisatorische Maßnahme zu dokumentieren. Wäre jeder Verantwortliche dazu verpflichtet, stets lückenlos nachweisen können zu müssen, dass er aktuell alle Pflichten der DS-GVO erfüllt und dass er auch in der Vergangenheit stets alle*

Pflichten erfüllt hat, verursachte dies darüber hinaus einen enormen bürokratischen Aufwand.

Grundrechtliche Grenzen:

Eine umfassend zu verstehende Meta-Nachweispflicht wäre ein unverhältnismäßiger Eingriff in die grundrechtlich geschützte Handlungsfreiheit des Einzelnen oder anderer Grundrechte, die durch die Verarbeitung in Anspruch genommen werden. Dies wäre vergleichbar mit der Pflicht eines jeden Autofahrers, nachweisen zu müssen, sich zu jeden Zeitpunkt an alle Verkehrsvorschriften (inkl. der Geschwindigkeitsbegrenzungen) gehalten zu haben.

Risikobasierter Ansatz [Kachel PK.17]:

Beschränkendes Element für die Nachweispflicht ist auch der risikobasierte Ansatz. Er gilt gemäß Art. 24 I 1 für alle technischen und organisatorischen Maßnahmen, die den Nachweis dafür erbringen sollen, dass die Verarbeitung „gemäß dieser Verordnung" erfolgt. Auch für die Nachweispflicht gilt somit, dass nur solche Nachweise zu erbringen sind, die unter Risikogesichtspunkten erforderlich und verhältnismäßig sind. Daher besteht eine Nachweispflicht nur in Bezug auf die risikogeneigtesten Verarbeitungen.

Grundsatz der Selbstbelastungfreiheit [Kachel L.10]:

Ein enormes Spannungsverhältnis besteht zwischen dem Nachweisenkönnenmüssen einerseits und dem Grundsatz der Selbstbelastungsfreiheit andererseits. Der Umstand, dass der Verantwortliche eine umfangreiche Dokumentation seiner Compliancebemühungen vornehmen muss, führt natürlich dazu, dass ein etwaiger Verstoß leichter sichtbar, leichter nachweisbar und leichter sanktionierbar ist. Dies ist wohl auch ein Zweck der Rechenschaftspflicht. Es ist jedoch im Rechtsstaat nicht selbstverständlich, dass sich der Verantwortliche im Rahmen einer von ihm geforderten Eigenüberwachung gegenüber Behörden selbst belasten (sozusagen „selbst ans Messer liefern") muss. Dies gilt auch für das Verhältnis des Verantwortlichen gegenüber den Datenschutzaufsichtsbehörden oder den Strafverfolgungsbehörden.

Beweislastverteilung im zivilrechtlichen Verfahren:

Fraglich ist, ob und inwieweit die Nachweispflichten der DS-GVO Einfluss auf die Darlegungs- und Beweislast im zivilrechtlichen Verfahren haben. Grundsätzlich ist jede Partei für die ihr günstigen Umstände darlegungs- und beweispflichtig. Der Gesetzgeber kann aber Beweiserleichterungen, gesetzliche Vermutungen, eine Beweislastumkehr oder eine Gefährdungshaftung zugunsten der einen oder anderen Seite festlegen. Dies könnte durch die Nachweispflichten der DS-GVO geschehen sein. Diesbezügliche Fragen sind aber durch die Rechtsprechung noch nicht entschieden.