
Dr. Markus Knasmüller

Allgemein beedeter und gerichtlich zertifizierter Sachverständiger für Informations- und Kommunikationstechnologie sowie für Glücksspiel; Abteilungsleiter Entwicklung, BMD Systemhaus GesmbH, Steyr

Erste Erfahrungen mit der Datenschutz-Grundverordnung für Sachverständige*

1. Einleitung

Mit 25. 5. 2018 ist die Datenschutz-Grundverordnung (DSGVO)¹ in Kraft getreten und schon lange davor war klar, dass die Arbeitsweise in allen Unternehmen – und natürlich auch der Sachverständigen – davon betroffen sein wird. So wichtig Datenschutz auch ist, so umstritten war die DSGVO und teilweise wurde vor dem Inkrafttreten richtiggehend eine Panikstimmung, insbesondere von verschiedenen Medien, aber auch Beratern, verbreitet. Dies vor allem wegen der hohen Strafandrohungen von bis zu € 20 Mio, wobei für große Konzerne sogar noch höhere Strafen vorgesehen sind (bis zu 4 % des jährlichen, weltweiten Konzernumsatzes).

Vorweg kann gesagt werden, dass zumindest in Österreich die hohen Strafen ausgeblieben sind. *De facto* gibt es wegen „üblicher“ Datenverarbeitungen noch gar keine rechtskräftige Strafe.² Einzig wegen Videoüberwachungen wurden bislang Strafen ausgesprochen, aber auch hier lag die bisher verhängte Höchststrafe nur bei € 4.800,- und damit in einem überschaubaren Rahmen. Dies wohl vor allem deshalb, weil der Gesetzgeber in § 11 Datenschutzgesetz (DSG) den Leitsatz „Beraten statt strafen“ ausgab (arg: „Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde ... insbesondere durch Verwarnen Gebrauch machen.“) und dadurch die eigentlich in der DSGVO vorgesehenen wirksamen, verhältnismäßigen und abschreckenden Strafen zumindest bei Erstvergehen vielfach wegfallen.

Wenn also auch prognostizierte Katastrophen ausgeblieben sind, so brachte die DSGVO dennoch eine Vielzahl an Vorschriften, deren Einhaltung häufig einen hohen Aufwand bedeutet, mit sich. Leider sind diese Vorschriften oft auch etwas „schwammig“ formuliert, was dazu führt, dass wesentliche Fragen (etwa ob der Sachverständige Verantwortlicher oder Auftragsverarbeiter im Sinne der DSGVO ist) immer noch nicht endgültig beantwortet sind. Dennoch hat das erste Jahr nach Einführung in vielen Punkten doch Klarheit gebracht oder zumindest kann ersten Bescheiden der Datenschutzbehörde eine Tendenz entnommen werden. Insofern ist es also durchaus sinnvoll, sich mit den ersten Erfahrungen, insbesondere Bezug nehmend auf die Tätigkeit der Sachverständigen, auseinanderzusetzen. Dies ist Ziel dieses Artikels.

2. Die wichtigsten Vorschriften

Die wichtigsten Punkte der DSGVO, die sich auf die Verarbeitung von personenbezogenen Daten bezieht (dazu gehören neben Datenfeldern in Software auch Excel- bzw Word-Dateien, E-Mails, Videos oder Fotos), sind:³

- Für jede Speicherung von Daten ist ein Rechtsgrund (zB gesetzliche Verpflichtung, Einwilligung, durchaus auch berechtigtes Interesse oder – wohl auch für Gerichtssachverständige interessant – Aufgaben im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt) erforderlich. Außerdem dürfen die Daten nur für den festgelegten Zweck verwendet und nur so lange gespeichert werden, wie es für den Zweck erforderlich ist. Das heißt, alle Daten müssen jedenfalls irgendwann wieder gelöscht werden.
- Unternehmen ab 250 Mitarbeitern sind zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten verpflichtet. Darin sind alle Anwendungen, mit denen personenbezogene Daten verarbeitet werden (also etwa eine Kundendatenbank, die Lohnverrechnung, aber auch eventuell einfache Excel-Tabellen) anzuführen und unter anderem ist zu beschreiben, welche Kategorien von Daten zu welchem Zweck verarbeitet werden. Auch kleinere Unternehmen müssen für einen Teil ihrer Anwendungen (etwa für die Lohnverrechnung) derartige Verzeichnisse führen.
- Recht auf Information: Wenn Daten einer Person verarbeitet werden, so muss die betroffene Person darüber informiert werden, sofern sich dies nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. Angemerkt sei, dass das Ärztegesetz 1998 nach § 3b Abs 2 Ärzte allerdings von dieser Verpflichtung ausnimmt.
- Recht auf Auskunft: Jede Person hat das Recht, Auskunft zu verlangen, ob über sie Daten verarbeitet werden und – falls ja – welche zu welchem Zweck und wie lange die Speicherdauer sein wird.
- Bei unrechtmäßiger Verarbeitung oder etwa auch bei widerrufener Einwilligung sind die Daten zu löschen. Macht die betroffene Person im Falle eines Verstoßes dieses Recht geltend und ist der Anspruch berechtigt,

* Dieser Aufsatz basiert auf einem Vortrag im Zuge des 29. Fortbildungsseminars für Sachverständige am Brandlhof im April 2019.

so sind die Daten unverzüglich zu löschen (theoretisch wohl sogar inklusive etwaiger Sicherungen, auch wenn hier § 4 DSGVO mit der Anmerkung, dass, falls nicht gelöscht werden kann, die Daten einzuschränken sind, für eine Erleichterung sorgt).

- Bei etwaigen Verletzungen des Datenschutzes, wenn etwa irrtümlich persönliche Daten für die Allgemeinheit ins Netz gestellt werden, aber auch bei einem Hackerangriff bzw sogar teilweise bei einer irrtümlich falsch versendeten E-Mail sind innerhalb von 72 Stunden die Behörden und bei voraussichtlich hohem Risiko auch die Betroffenen zu verständigen.
- Für die Speicherung der Daten in Drittländer gelten besondere, sehr strenge Vorschriften.

Wesentlich ist dabei, dass unter personenbezogenen Daten alle Angaben über natürliche Personen, deren Identität identifiziert oder identifizierbar ist, verstanden werden. Dazu gehören auch triviale Dinge (wie Namen, Adressen, Telefonnummern, aber auch IP-Adressen und Kfz-Kennzeichen). Es müssen also nicht „sensible“ Daten (wie biometrische Daten, Gesundheitsdaten oder Angaben zur Sexualität) sein, damit diese unter die DSGVO fallen, sondern alle Daten sind betroffen. Jene „sensiblen“ Daten, die die DSGVO als „*besondere Kategorie personenbezogener Daten*“ bezeichnet, sind allerdings besonders geschützt (etwa kann in diesem Fall das berechtigte Interesse nicht als Speicherungsgrund geltend gemacht werden).

3. Verantwortlicher oder Auftragsverarbeiter

Ein wesentlicher Punkt bei diesen Vorschriften ist, dass einige davon (etwa die gesamten Transparenzrechte, also das Recht auf Information oder das Recht auf Auskunft) nur durch den Verantwortlichen, nicht aber durch den Auftragsverarbeiter zu erfüllen sind. Insbesondere treffen die Rechte auf Information und Auskunft nicht den Auftragsverarbeiter.

Nur wo liegt der Unterschied zwischen diesen beiden Gruppen im Sinne der DSGVO?

- Verantwortlicher entscheidet alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten.
- Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen.
- Verarbeitung ist dabei jeder Vorgang im Zusammenhang mit persönlichen Daten (wie Erheben, Erfassen, Organisieren, Ordnen, Speichern, Verändern, Auslesen, Abfragen, Verwenden, aber auch Löschen).

Diese Definitionen sind dabei tatsächlich etwas unpräzise und lassen großen Spielraum. Der Hauptverband der allgemein beeideten und gerichtlich zertifizierten Sachverständigen vertritt dabei (gestützt auf ein Rechtsgutachten und auch auf die Erläuterungen zu § 83 GOG in der Fassung der Novelle BGBl I 2018/32)⁴ die Ansicht, dass

Gerichtssachverständige bei Erstattung von Gutachten im Auftrag eines Gerichts oder einer Staatsanwaltschaft, aber wohl auch im privaten Auftrag bis zur Erfüllung des Auftrags im Regelfall nur Auftragsverarbeiter sind. Dies, da Gerichtssachverständige hinsichtlich des Zwecks und des sich daraus ergebenden Umfangs der Datenverarbeitung an den Gutachtensauftrag gebunden sind und daher tatsächlich nur in diesem Rahmen über die Frage, welche Daten konkret verarbeitet werden und mit welchen technischen Mittel dies geschieht, entscheiden.⁵

Hingegen hat das BVwG in seinem Erkenntnis vom 27. 9. 2018, W214 2127449-1, einen anderen Standpunkt vertreten. Demnach wäre der Sachverständige zumindest gemeinsam mit dem Gericht datenschutzrechtlicher Verantwortlicher, da selbständig und eigenverantwortlich über die Mittel entschieden wird.

Es wird hierzu die höchstgerichtliche Rechtsprechung abzuwarten sein, um diese Frage endgültig zu klären, weswegen es sinnvoll ist, auf beide Varianten kurz einzugehen, denn jedenfalls hat auch ein Auftragsverarbeiter natürlich ein Mitwirkungsrecht bei der Erfüllung der Transparenzpflichten.

Neben den unterschiedlichen Verpflichtungen, die Auftragsverarbeiter und Verantwortliche treffen, ist für einen Auftragsverarbeiter auch noch Folgendes zu beachten:

- Dieser muss garantieren, dass Verarbeitung im Einklang mit der DSGVO erfolgt.
- Dritte werden nicht hinzugezogen, außer bei Verständigung und Zustimmung des Verantwortlichen.
- Ein klarer Vertrag mit entsprechenden Bestimmungen muss bestehen, sofern nicht ein anderes Rechtsinstrument (im Falle eines Gerichtsgutachtens wohl der Gutachtensauftrag iVm der ZPO, der StPO etc) die Grundlage für die Verarbeitung schafft.
- Nach Abschluss der Arbeiten erfolgt eine Löschung der Daten, sofern nicht gesetzliche Verpflichtung für eine längere Aufbewahrung besteht.
- Die Verarbeitung der Daten erfolgt ausschließlich auf Weisung des Verantwortlichen.

Zumindest das Recht auf Auskunft würde der Sachverständige auch dann, wenn er als Verantwortlicher gelten sollte, wohl nur sehr eingeschränkt erfüllen müssen. Denn in vielen Fällen wäre wohl die Verschwiegenheitspflicht höherwertiger.

4. Datenschutz-Folgenabschätzung

Ein Punkt, der zum Zeitpunkt des Inkrafttretens der DSGVO auch etwas unsicher war, war, wann Datenschutz-Folgenabschätzungen notwendig sind. Grundsätzlich gilt nach Art 35 DSGVO, dass, wenn 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 hat, der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen hat.

Um klarer zu definieren, wann derartige Folgenabschätzungen nötig sind, hat die Datenschutzbehörde eine sogenannte White List (DSFA-AV)⁶ und auch eine Black List (DSFA-V)⁷ herausgegeben. Die DSFA-AV regelt dabei Ausnahmen von der Datenschutz-Folgenabschätzung, beschreibt also Fälle, in denen jedenfalls keine Datenschutz-Folgenabschätzung notwendig ist.

Die in dieser Verordnung stehende Ausnahme für die Datenverarbeitung von rechtsberatenden und unternehmensberatenden Berufen (wie einzelne Rechtsanwälte, Notare, Patentanwälte, Wirtschaftstreuhänder, Steuerberater und Unternehmensberater im Rahmen ihrer Berufsausübung) legt nahe, dass auch der Sachverständige im Regelfall keine Datenschutz-Folgenabschätzung vorzunehmen haben wird, obwohl eine im Rahmen der Begutachtung der Verordnung abgegebene Stellungnahme des Hauptverbandes, die Datenverarbeitung von gerichtlich zertifizierten Sachverständigen generell auszunehmen, nicht im Wortlaut aufgegriffen wurde.

Auch die DSFA-V enthält keinerlei Regelungen, die zumindest für die üblichen Sachverständigentätigkeiten eine andere Einschätzung erforderlich machen würden.

5. Wesentliche Entscheidungen

In diesem Abschnitt soll auf einige relevante Entscheidungen, die vor allem seitens der österreichischen Datenschutzbehörde veröffentlicht worden sind, eingegangen werden.

Eine der umfassendsten Entscheidungen bisher war der Bescheid der Datenschutzbehörde vom 16. 11. 2018, DSB-D213.692.0001-DSB/2018. Hier wurden aufgrund einer Meldung einer Datenschutzverletzung behördenseitig Untersuchungen eingeleitet und in weiterer Folge wurde eine Reihe von interessanten Beschlüssen gefasst. Neben der Festlegung, dass bei einer Allergieklinik mit unter anderem 17 Ärzten jedenfalls eine umfangreiche Verarbeitung besonderer Kategorien von Daten besteht und deswegen verpflichtend ein Datenschutzbeauftragter bestellt werden muss, wurden auch einige Einwilligungen als rechtswidrig aufgehoben. Dies betraf insbesondere Einwilligungen, die im Rahmen eines Vertrages abgegeben wurden, obwohl diese für die Erfüllung des Vertrages nicht notwendig waren, sowie solche, die Zustimmungen betrafen, für die laut DSGVO keine Zustimmungen notwendig sind (wie etwa das Hinzuziehen von Auftragsverarbeitern; dies ist eine Entscheidung, die ausschließlich der Verantwortliche zu treffen hat). Besonders interessant an dieser Entscheidung ist aber auch, dass demnach aus der DSGVO auch mittelbar keine Verpflichtung, Daten verschlüsselt zu übermitteln, abgeleitet werden kann.

In diese Richtung geht auch der Bescheid der Datenschutzbehörde vom 13. 9. 2018, DSB-D123.070/0005-DSB/2018, wonach aus der DSGVO kein Recht abzuleiten ist, durch das eine betroffene Person spezifische Datensicherheitsmaßnahmen von einem Verantwortlichen verlangen könnte. So kann von dieser etwa keine Pseudonymisierung verlangt werden.

Relevant für Sachverständige sind auch die bisher bereits ergangenen Entscheidungen betreffend die Aufbewahrungsfristen. Nach Punkt 2.10.11 der Landesregeln wird derzeit empfohlen, zum eigenen Gebrauch angefertigte Aufzeichnungen und Unterlagen nach Beendigung der Gutachtertätigkeit 10 Jahre aufzubewahren. Aufgrund einiger bisheriger Entscheidungen ist anzunehmen, dass eine derartige lange Aufbewahrungsfrist nur aufgrund konkreter Bedürfnisse vertretbar sein wird. Der Hauptverband wird voraussichtlich ein Rechtsgutachten in Auftrag geben, das beruhend auf dem Gesetz und den bisherigen Entscheidungen eine neue Empfehlung für die Landesregeln ausarbeiten wird.

Interessant ist abschließend auch noch das Urteil des OLG Frankfurt vom 12. 2. 2019, 11 U 114/17, in dem es um die Weitergabe eines Kfz-Privatgutachtens (inklusive von Lichtbildern) des Versicherungsnehmers an einen anderen Sachverständigen zwecks Überprüfung ging. Das Gericht stellte fest, dass dies nicht gegen die DSGVO verstößt, sondern die Versicherung die Daten des Versicherten und dessen Kfz zur Schadensregulierung speichern darf. Dies darf auch eine von ihr zu Kontrollzwecken beauftragte Stelle (also etwa ein weiterer Sachverständiger) im Rahmen der Auftragsdatenverwaltung.

6. Checkliste und Zusammenfassung

Zusammenfassend kann festgehalten werden, dass die Hauptbefürchtung im Zusammenhang mit der DSGVO, nämlich hohe Strafen, bislang zum Glück ausgeblieben ist. Dennoch soll dies aber natürlich kein Grund sein, sich nicht auch weiterhin intensiv Gedanken um den Datenschutz zu machen. Die nachfolgende Checkliste kann dafür eine Richtlinie sein. Wenngleich viele der Punkte wohl bereits seit der Einführung der DSGVO erfüllt sein müssten, so ist es dennoch sinnvoll, laufend die Punkte zu kontrollieren, ob sie auch noch erfüllt sind:

- Sofern die Sachverständigentätigkeit nicht durch einen einzelnen Sachverständigen vorgenommen wird, sondern es sich beispielsweise um ein Sachverständigenbüro handelt, so ist ein Verantwortlicher für den Bereich Datenschutz zu definieren. Diese Person hat etwa die Aufgabe, Auskunftersuchen zu bearbeiten oder auch etwaige Meldungen von Datenschutzverletzungen an die Behörde zu veranlassen.
- Es ist zu überlegen, welche Daten verarbeitet werden. Zu diesem Zweck ist ein Verzeichnis der Verarbeitungstätigkeiten zu führen, wobei folgende Punkte zu berücksichtigen sind:

- Welche Anwendungen?
- Welche Zwecke?
- Rechtsgrundlagen für die Speicherung von personenbezogenen Daten.
- Sind Daten besonderer Kategorie darunter?
- Sind Kinder davon betroffen (in Österreich Personen unter 16 Jahren)?

Die Pflicht zur Führung dieses Verzeichnisses gilt zwar bei Unternehmen erst ab 250 Mitarbeitern für alle Verarbeitungstätigkeiten, ansonsten nur, wenn die Verarbeitung nicht nur gelegentlich erfolgt oder besondere Datenkategorien beinhaltet (oder ein Risiko für die Rechte und Freiheiten der betroffenen Person birgt). Dennoch ist das Führen dieses Verzeichnisses wohl immer zu empfehlen, alleine schon deshalb, weil etwa eine Auskunft, basierend auf diesem Verzeichnis, einfacher erfolgen kann. Besonders wesentlich ist, dass dieses Verzeichnis laufend kontrolliert wird, insbesondere dann, wenn neue Anwendungen hinzukommen oder wesentliche Änderungen durchgeführt werden.

- Wird mit Auftragsverarbeitern zusammengearbeitet, müssen in diesem Falle entsprechende Vereinbarungen unterzeichnet werden. Grundsätzlich muss diese Frage wohl bei jedem neuen Lieferanten überlegt werden.
- Sämtliche Verträge, allgemeinen Geschäftsbedingungen, aber auch Websites sind bei Änderungen in Bezug auf Datenschutzpunkte zu kontrollieren.
- Die Informationspflicht sollte durch entsprechende Datenschutzerklärungen auf der Website erfüllt werden.
- Besteht Datenverkehr mit dem EWR-Ausland? Diese Frage sollte insbesondere bei neuen Kunden oder Lieferanten hinterfragt werden, weil diesbezüglich etwa Änderungen notwendig sein könnten. Grundsätzlich gestattet die DSGVO die Speicherung von personenbezogenen Daten nämlich nur im EWR-Raum oder in Staaten mit vergleichbar strengen Datenschutzbestimmungen (wie etwa die Schweiz, Kanada oder Japan). In anderen Ländern darf die Speicherung nur unter ge-

wissen Voraussetzungen (etwa ausdrückliche Einwilligung) erfolgen.

- Die Umsetzung angemessener Sicherheitsmaßnahmen sollte vorgenommen werden.
- Verschwiegenheitserklärung: Jeder Mitarbeiter sollte eine Verschwiegenheitserklärung unterzeichnen. Diese kann einfach formuliert werden, etwa indem der Text des § 6 DSGVO unterschrieben wird.
- Mitarbeiterschulungen (zB durch Webinare) sollen vorgenommen und dokumentiert werden.

Wichtig ist abschließend, dass, auch wenn dieser Artikel in einigen Punkten (insbesondere in Bezug auf die Strafandrohung) vielleicht für Entspannung sorgen wird, es doch wesentlich ist, dem Datenschutz als Sachverständiger einen hohen Stellenwert zukommen zu lassen. Denn unzweifelhaft ist eine Tätigkeit wie die eines Sachverständigen, die also mit dem Verlust von Vertraulichkeit von Berufsgeheimnissen verbunden ist, eine dem Erwägungsgrund 85 der DSGVO nach mit „hohem Risiko“ den Datenschutz betreffende Tätigkeit.

Anmerkungen:

- ¹ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABI L 119 vom 4. 5. 2016, S 1.
- ² Stand: 30. 9. 2019.
- ³ Siehe auch *Schmidt*, Datenschutz bei Sachverständigenstätigkeit, SV 2018/2, 68.
- ⁴ ErlRV 65 BlgNR 26. GP, 150.
- ⁵ *Guggenbichler*, Bundesverwaltungsgericht zur datenschutzrechtlichen Stellung von Gerichtssachverständigen, SV 2019/1, 3.
- ⁶ Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung (DSFA-AV), BGBl II 2018/108.
- ⁷ Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V), BGBl II 2018/278.

Korrespondenz:

Dr. Markus Knasmüller
Edelhof 45, 3350 Haag
E-Mail: markus@knasmueller.at