

LANDTAG

NORDRHEIN-WESTFALEN
16. WAHLPERIODE**STELLUNGNAHME
16/537**

Alle Abg

Unsere Antworten zum Fragenkatalog des Landtags NRW:

- 1 *1. Halten Sie die Datenschutz-Grundverordnung für grundsätzlich zulässig*
- 2 *hinsichtlich der Regelungskompetenz der EU?*
- 3 Keine Angabe
- 4 *2. Halten Sie die Rechtsform der Verordnung für sinnvoll und angemessen*
- 5 *oder hätte man Ihres Erachtens eher auf eine Weiterentwicklung der*
- 6 *bestehenden Datenschutzrichtlinie setzen sollen?*
- 7 Die Rechtsform der Verordnung schafft ein europaweit einheitliches
- 8 Datenschutzrecht. Dies dient den Verbraucherinnen und Verbrauchern,
- 9 weil es ihnen Gewissheit über die Regeln der Datenverarbeitung auch in
- 10 der gesamten EU gibt. Außerdem wird durch ein europaweit
- 11 harmonisches Datenschutzrecht das Gewicht des Datenschutzes in der
- 12 EU hinsichtlich der Datenverarbeitung durch Unternehmen in Drittstaaten
- 13 (insbesondere großen US-amerikanischen Firmen) gestärkt. Gerade
- 14 Artikel 3 (territorial scope) zeigt hier eindeutig den Willen der Kommission,
- 15 die Rechte der Bürgerinnen und Bürger innerhalb der EU vor solch
- 16 grenzüberschreitender Datenverarbeitung zu stärken. Allerdings sollte Art.
- 17 3, Abs. 2, Satz a nicht dahingehend interpretiert werden, dass die
- 18 Datenschutzverordnung nur auf „kostenpflichtige“ Dienste angewendet
- 19 werden kann.
- 20 Eine Weiterentwicklung der Richtlinie, die immerhin aus dem Jahr 1995
- 21 stammt, hätte diesen Ansatz, demzufolge ein einheitliches
- 22 Datenschutzgesetz mehr Durchsetzungskraft und vor allem mehr
- 23 Rechtssicherheit bietet, aufgrund der nationalstaatlichen
- 24 Regelungsspielräume eher geschwächt.

25 3. Welche konkreten Verbesserungen sehen Sie hinsichtlich der
26 Europäischen Datenschutzreform für die Bereiche a) Datenschutz im
27 Internet b) Arbeitnehmerdatenschutz c) Verbraucherdatenschutz?

28 Ad 3a) Der Kommissionsvorschlag regelt durch Art. 3 auch Fälle, in denen
29 die datenverarbeitende Stelle nicht innerhalb der EU angesiedelt ist, wohl
30 aber die betroffene Person. Diese konkrete Verbesserung ist sehr zu
31 begrüßen, allerdings muss sichergestellt werden, dass sie auch dann gilt,
32 wenn die datenverarbeitende Stelle „kostenlose“ Dienste oder Güter
33 anbietet.

34 Die „explizite Einwilligung“, wie sie in Art. 6, Abs. 1, Satz a i. V. m. Art. 4,
35 Abs. 8 geregelt ist, würde eine sehr große Verbesserung – offline wie
36 online – für die Verbraucherinnen und Verbraucher bedeuten. Gerade im
37 Zuge der Debatte um das Meldegesetz hat der vzbv nochmal deutlich
38 gemacht, wie oft Einwilligungen in die Datenverarbeitung „erschlichen“
39 werden – durch versteckte Voreinstellungen oder Ähnlichem.
40 ([https://www.foebud.org/datenschutz-](https://www.foebud.org/datenschutz-buergerrechte/vzbv_hintergrund_unwirksame_einwilligungen_231012_print.pdf)
41 [buergerrechte/vzbv_hintergrund_unwirksame_einwilligungen_231012_prin](https://www.foebud.org/datenschutz-buergerrechte/vzbv_hintergrund_unwirksame_einwilligungen_231012_print.pdf)
42 [t.pdf](https://www.foebud.org/datenschutz-buergerrechte/vzbv_hintergrund_unwirksame_einwilligungen_231012_print.pdf))

43 Die Ausgestaltung der Einwilligung als „explizite“ Einwilligung muss
44 deshalb bestehen bleiben und darf nicht in „informierte“ oder gar „implizite“
45 Einwilligung geändert werden. Aus den gleichen Gründen muss die
46 Datenverarbeitung aufgrund des „legitimen Interesses“ der
47 datenverarbeitenden Stelle eingeschränkt werden. Art. 6, Abs. 1, Satz f
48 wägt die Grundrechte der betroffenen Personen gegen die legitimen
49 Interessen der datenverarbeitenden Stelle ab. Diese Abwägung ist
50 allerdings höchst problematisch, weil sie von der datenverarbeitenden
51 Stelle selbst vorgenommen wird und dementsprechend nicht ausgewogen
52 sein kann.

53 Durch das Recht auf Datenübertragbarkeit (Art. 18) wird das
54 Datenschutzrecht im Internet innovativ weiterentwickelt. Dieses Recht
55 bietet Nutzerinnen und Nutzern von sozialen Netzwerken oder ähnlichen
56 Diensten die Möglichkeit, ihre einmal aufgebaute „persona“ mitzunehmen
57 und bei Wettbewerbern wiederzuverwenden. Dadurch sehen wir die
58 Möglichkeit, dass sich datenschutzfreundlichere Wettbewerber etablieren
59 können und so einen Anreiz für europäische Innovationen.

60 Ad 3b) Die Ausführungen in Art. 35, die die Berufung eines
61 Datenschutzbeauftragten vorschreiben bringen keine Verbesserungen.
62 (Siehe nächste Frage)

63 Ad 3c) Der Verbraucherdatenschutz wird besonders durch die Erfordernis
64 der „expliziten Zustimmung“ sowohl online wie offline gestärkt. (s. Ad 3a))
65 Durch die Stärkung der Auskunftsrechte in Art. 15 können
66 Verbraucherinnen und Verbraucher schnell, einfach und umfangreich
67 Auskunft über die von ihnen verarbeiteten Daten bekommen. Der Entwurf
68 gibt der Kommission allerdings das Recht im Rahmen eines „delegated
69 acts“ die Kriterien weiter auszuführen – hier braucht es eine Regelung
70 innerhalb der Verordnung und nicht erst nachgeordnet durch die
71 Kommission.

72 *4. In welchen Bereichen – insbesondere mit Blick auf die unter Frage 3*
73 *genannten Spezialgebiete – sehen Sie die Gefahr einer Absenkung von*
74 *Datenschutz-Standards gegenüber dem deutschen Datenschutzrecht?*

75 Ad 4a) Internet: Artikel 20 (Maßnahmen, die auf Profiling beruhen) ist
76 eindeutig zu weit gefasst. Betroffene Personen haben kein Recht, dem
77 Profiling selbst zu widersprechen, sondern nur den darauf beruhenden
78 Maßnahmen. Absatz 2 schränkt diesen Widerspruch dann noch weiter ein.
79 Hier bedarf es einer verbraucher- und bürgerfreundlichen Regelung, die
80 das automatisierte Verarbeiten von Daten grundrechtskonform
81 ausgestaltet.

82 Eine grundlegende Gefahr ist die Absenkung des Datenschutzes durch
83 eine zu weiche Definition von „betroffener Person“ oder
84 „personenbezogene Daten“. Dabei muss unbedingt darauf geachtet
85 werden, dass personenbeziehbare Daten genauso behandelt werden wie
86 personenbezogene Daten. Das heißt, dass Art. 4, Abs. 1 genau geprüft
87 werden muss hinsichtlich der Mittel, „die der für die Verarbeitung
88 Verantwortliche oder jede sonstige natürliche oder juristische Person nach
89 allgemeinem Ermessen aller Voraussicht nach einsetzen würde .“

90 Das TMG sieht vor, dass man Internet-Dienste immer auch unter
91 Pseudonym verwenden können muss. Diese Regelung sollte explizit auch
92 in die Verordnung aufgenommen werden, ohne dass daraus ein
93 niedrigeres Schutzniveau für pseudonyme Daten entsteht.

94 Ad 4b) Arbeitnehmer: Artikel 35 bringt eine Verschlechterung in Bezug auf
95 den Datenschutzbeauftragten in Unternehmen. Dieser wäre nach
96 Kommissionsentwurf nur noch erforderlich, wenn die Kerntätigkeit des
97 Unternehmens in der Datenverarbeitung liegt oder wenn das
98 Unternehmen mehr als 250 Mitarbeiter hat. Die Regelung zielt natürlich
99 auf KMU, dennoch ist es nicht einzusehen, warum der
100 Datenschutzbeauftragte in Unternehmen, der sich in Deutschland auch bei
101 KMU bewährt hat, entfallen soll.

102 Ad 4c) Verbraucher: Die Ausweitung der Datenverarbeitung aufgrund des
103 „legitimen Interesses“ (Art. 6, Abs. 1, Satz f) muss unbedingt
104 eingeschränkt werden! Für Verbraucherinnen und Verbraucher ist nicht
105 einzusehen, wer ein „legitimes Interesse“ an ihren Daten hat und wie
106 Unternehmen die Abwägung selbst gegenüber den Rechten der
107 Verbraucher objektiv vornehmen können. Der Ansatz im Entwurf des
108 Berichterstatters Jan Philipp Albrecht bietet hier eine mögliche Lösung,
109 derzufolge Unternehmen die Gründe, warum sie davon ausgehen, dass
110 ihre legitimes Interesse überwiegt, vorab veröffentlichen müssen.
111 Außerdem werden Kategorien etabliert, bei denen ein legitimes Interesse

112 die Abwägung gegen die Grundrechte der betroffenen Personen nie
113 überwiegt. Allerdings sind diese auch noch sehr weit gefasst.

114 *5. Welche Regelungen des deutschen und des Nordrhein-Westfälischen*
115 *Datenschutzrechts sollten aus Ihrer Sicht unbedingt erhalten bleiben?*

116 Der Grundsatz im deutschen Datenschutzrecht, der personenbeziehbare
117 Daten zu personenbezogenen Daten macht, sollte genauso wie das
118 Verbot mit Erlaubnisvorbehalt zur Datenverarbeitung unbedingt erhalten
119 bleiben. Außerdem darf die Einheitlichkeit der Regelungen nicht
120 unterlaufen werden. Verschiedene Stellen fordern in letzter Zeit,
121 Regelungen die sich nach verschiedenen Risikostufen der verarbeiteten
122 Daten richten. Solche Forderungen sind nicht praxistauglich, weil sie für
123 Verbraucherinnen und Verbraucher undurchsichtig sind. Für den
124 Bürokratieabbau, den sich die Wirtschaft wünscht und gleichzeitig solche
125 Forderungen erhebt, ist nicht zu verstehen, warum solche Fall zu Fall
126 Risikoabschätzungen Bürokratieabbau leisten sollen.

127 *6. Welche Durchsetzungsdefizite sehen Sie im heutigen*
128 *Datenschutzrecht? Inwiefern werden diese durch die Europäische*
129 *Datenschutzreform gemindert oder beseitigt?*

130 Die territoriale Anwendung ist in Zeiten vernetzter und globalisierter
131 Datenverarbeitung ein großes Problem, das durch Artikel 3 der
132 Datenschutzverordnung entsprechend angegangen wird. Demzufolge
133 müssen Unternehmen sich auch dann dem Europäischen
134 Datenschutzrecht unterwerfen, wenn sich ihre Dienste und Services an
135 europäische Bürger richten. Dabei muss sichergestellt werden, dass das
136 auch dann gilt, wenn die Services und Dienste „kostenlos“, also nicht mit
137 Geld bezahlt, sind.

138 Ein weiteres sehr großes Problem sind die Strafzahlungen, die nach
139 deutschem Datenschutzrecht auf 300.000 Euro begrenzt sind – zwar
140 können diese überschritten werden, jedoch kommt dies in der Praxis

141 selten vor. Im Kommissionsentwurf wird dieser Betrag relativ zum
142 weltweiten Jahresumsatz (zwischen 0,5 bis 2 %) vom betroffenen
143 Unternehmen festgesetzt, was als Strafzahlung viel effektiver ist.

144 Um Durchsetzungsdefizite noch weiter zu mindern, sollte für
145 Datenschutzbehörden eine Mindestaustattung an Personal und Mitteln
146 festgeschrieben werden. Gleichzeitig sollte die Ernennung nicht wie im
147 Kommissionsvorschlag von Parlament oder Regierung erfolgen, sondern
148 nur von den nationalen Parlamenten.

149 *7. Welche Vor- und Nachteile sehen Sie in den durch die Europäische*
150 *Datenschutzreform vorgesehenen Veränderungen in der*
151 *Datenschutzaufsicht*

152 Die in Kapitel VI und VII ergriffenen Maßnahmen in der
153 Datenschutzaufsicht sind mit einigen Einschränkungen positiv zu sehen.
154 Die Kooperationen untereinander werden gestärkt und bei Untätigkeit
155 einer nationalen Behörde kann die Behörde eines anderen Staates
156 provisorische Maßnahmen für sich ergreifen. Die Festsetzung erhöhter
157 Strafzahlungen (s.o.) bietet zudem einen weiteren Vorteil.

158 *8. Halten Sie es für sinnvoll, dass die Verordnung auch öffentliche Stellen*
159 *erfassen soll und damit nach derzeitigem Entwurfsstand für öffentliche*
160 *(auch hoheitlich im Bereich der Eingriffsverwaltung handelnde) Stellen*
161 *gleiche Regelungen gelten würden, wie für Private und wirtschaftlich*
162 *Handelnde? Halten Sie eine Differenzierung für sinnvoll und erforderlich?*

163 k.A.

164 *9. Wie beurteilen Sie die Auswirkungen der unterschiedlichen Regelungen*
165 *für die Gefahrenabwehr (Verordnung: nicht-straftatenbezogen, Richtlinie:*
166 *straftatenbezogen)? Lässt sich insbesondere in der Praxis sachgerecht*
167 *abgrenzen?*

168 k.A.

169 *10. Wie beurteilen die Sachverständigen den Entwurf der Kommission für*
170 *eine EU-Datenschutz-Grundverordnung im Vergleich zur geltenden*
171 *Rechtslage?*

172 Siehe zu 3. und 4.

173 *11. Ist der Entwurf der Kommission mit dem Subsidiaritätsprinzip (Art. 5*
174 *Abs. 3 EUV) vereinbar?*

175 k.A.

176 *12. Wie beurteilen die Sachverständigen die Umsetzbarkeit der in dem*
177 *Entwurf für die EU-Datenschutz-Grundverordnung enthaltenen Vorgaben*
178 *für die Datenverarbeitung in Unternehmen?*

179 Die Datenschutzgrundverordnung wird europa- und weltweit Standards für
180 den Datenschutz setzen und die Vorgaben für Unternehmen zur
181 Datenverarbeitung neu justieren und ins digitale Zeitalter portieren.
182 Besonders die Gründe für Datenverarbeitung und die Informations- und
183 Auskunftsrechte sind davon betroffen – Rechte, die den Unternehmen
184 zunächst Kosten verursachen könnten, auf lange Sicht aber das Vertrauen
185 der Bürgerinnen und Bürger stärken werden. Dadurch können
186 datenschutzfreundlichere Dienste und Services entstehen, so dass
187 Europa hier – ähnlich wie im Umweltschutz – Vorreiter und
188 Innovationsmotor werden kann. Datenschutz sollte demnach nicht als
189 Bürde, sondern als Innovationsanreiz gesehen werden.

190 *13. Wie beurteilen die Sachverständigen die in Ziffer II.5 des Antrags*
191 *erhobene Forderung, wonach die Kontrolle einzelstaatlicher Grundrechte*
192 *den nationale Verfassungsgerichten erhalten bleiben soll, vor dem*
193 *Hintergrund, dass das Unionsrecht ohnehin keine Kontrolle nationaler*
194 *Grundrechte durch den Gerichtshof der Europäischen Union vorsieht?*

195 k.A.

196 *14. Wie beurteilen die Sachverständigen die Regelung des Datenschutzes*
197 *sowohl für öffentliche als auch für nichtöffentliche Stellen in ein und*
198 *demselben Rechtsetzungsakt, obgleich sich diese Bereiche erheblich*
199 *voneinander unterscheiden?*

200 k.A.

201 *15. Wie beurteilen die Sachverständigen die Vielzahl von*
202 *Einzelermächtigungen zu bestimmten Sachbereichen des*
203 *Datenschutzrechts zu Gunsten der Kommission, so dass das europäische*
204 *Parlament weitgehend aus der Mitverantwortung für das Datenschutzrecht*
205 *genommen wird?*

206 Diese Regelung ist zurecht schon von vielen Seiten kritisiert worden und
207 auch wir sehen darin eine Umgehung demokratischer Prozesse auf EU-
208 Ebene. Die Einzelermächtigungen sollten – sofern sie nicht in der
209 Datenschutzverordnung geregelt werden können – unbedingt vom
210 Parlament bestimmt werden.

211 *16. Welche Anwendungslücken der Datenschutzgrundverordnung*
212 *bestehen im Hinblick auf die Datenerhebung und -nutzung durch*
213 *Unternehmen ohne Sitz in der EU, die zudem aufgrund des gewählten*
214 *Regelungsinstruments der Verordnung durch die Mitgliedstaaten nicht zu*
215 *beheben wären?*

216 Die in der Frage angesprochene Regelung des räumlichen
217 Anwendungsbereichs findet sich in Art. 3 Abs. 2. Danach unterfällt die
218 Verarbeitung von EU-Bürger-Daten im Ausland nur in 2 Fällen der
219 Verordnung: a) Anbieten von Waren und Dienstleistungen, b)
220 Beobachtung ihres Verhaltens. Das könnte sehr Wichtiges nicht erfassen:
221 Was ist z.B. mit unentgeltlichen Diensten? Sind das „Dienstleistungen“ im
222 Sinne von oben a)? Besser wäre es deshalb statt nur „Dienstleistungen“
223 auch „Dienste“ oder „entgeltliche und unentgeltliche Dienstleistungen“
224 aufzunehmen. Auch b) ist zu eng formuliert. Das Wort „dienen“ erfasst

225 nicht beiläufige, nicht-primär intendierte Beobachtungen. Statt „der
226 Beobachtung ihres Verhaltens dient“ sollte es heißen: „der Beobachtung
227 ihres Verhaltens dient oder eine solche ermöglicht“

228 *17. Schließt die in der Datenschutzgrundverordnung enthaltene*
229 *Legaldefinition des Begriffs der „personenbezogenen Daten“ bestimmte*
230 *Bereiche, die bisher nach mitgliedstaatlichem Recht dem*
231 *Datenschutzrecht unterlagen – wie z.B. die Videoüberwachung – vom*
232 *Anwendungsbereich der Datenschutzverordnungen aus?*

233 Artikel 4, Abs. 1 und 2 und die Erwägungsgründe 23 und 24 umfassen
234 unserer Ansicht nach nicht klar, ob etwa Videoüberwachung mit in den
235 Anwendungsbereich der Datenschutzverordnung fällt. Dies sollte aber auf
236 jeden Fall sichergestellt werden. Insgesamt ist sicherzustellen, dass in den
237 erwähnten Artikeln und Erwägungsgründen auf jeden Fall das Prinzip
238 „personenbeziehbare Daten sind personenbezogene Daten“ erhalten
239 bleibt – also dass etwa auch IP-Adressen, Cookies oder RFID-Tags mit
240 eindeutigen Nummern immer als personenbezogene Daten gelten.

241 *18. Welche Rechtsetzungsbefugnisse verblieben den Mitgliedstaaten nach*
242 *Inkrafttreten der Verordnungen im Bereich des Datenschutzes?*

243 Den Mitgliedstaaten bleiben kaum noch Rechtsetzungsbefugnisse, wie
244 sich insbesondere aus einem Umkehrschluss zu Art. 80, 82, 84 ergibt.
245 Artikel 21 gewährleistet nur das Recht der Mitgliedstaaten,
246 Einschränkungen der Grundsätze in Artikel 5 sowie Beschränkungen von
247 Datenschutzrechten im Sinne der Artikel 11 bis 20 und Artikel 32
248 beizubehalten oder einzuführen, gibt den Staaten also keine Befugnis für
249 einen erweiterten Datenschutz. Einige wenige Rechtsetzungsbefugnisse
250 bleiben den Mitgliedstaaten beim Arbeitnehmerdatenschutz, beim
251 Gesundheitsdatenschutz und bei der Datenverarbeitung für statistische,
252 historische und wissenschaftliche Zwecke.

253 19. Welche Auswirkungen erwarten die Sachverständigen hinsichtlich des
254 zu erwartenden Verwaltungs- und Kontrollaufwands nach Maßgabe der
255 Daten- schutzgrundverordnung auf kleine und mittelständische
256 Unternehmen (KMU)?

257 k.A.

258 20. Wie bewerten Sie das angestrebte Datenschutzniveau der
259 Grundverordnung im Vergleich zum Richtlinienentwurf für den
260 Sicherheitsbereich, insbesondere vor dem Hintergrund der mitunter
261 unspezifischen Formulierungen der datenschutzrechtlichen Vorgaben für
262 Polizei- und Justizbehörden?

263 k.A.

264 21. Wie ist Ihrer Ansicht nach die im Richtlinienvorschlag vorgesehene
265 „Erleichterung der Datenübermittlung an Drittländer und internationale
266 Organisationen“ – man denke hier an den Zugriff US-amerikanischer
267 Behörden auf europäische Fluggastdaten – mit der Gewährleistung eines
268 hohen Datenschutzniveaus vereinbar? Bedarf es hier Ihrer Ansicht nach
269 einer genaueren Definition und Begründung der vorgesehenen
270 „Erleichterung“?

271 Keine Angabe zum Richtlinienvorschlag, aber auch im Entwurf der
272 Verordnung ist die Datenübermittlung an Drittländer sehr problematisch
273 geregelt und darf in viel zu großem Umfang stattfinden. Dass dies
274 aufgrund eines starken Lobby-Interesses aufgeweicht wurde, zeigt auch
275 der geleakte Kommissions-Entwurf vom Dezember 2011, in dem die
276 Datenübermittlung an Drittstaaten wesentlich eingeschränkter und
277 verbraucherfreundlicher geregelt war.

278 22. Wie bewerten Sie die Vielzahl der delegierten Rechtsakte und
279 Durchführungsrechtsakte in der Datenschutz-Grundverordnung, welche
280 der Kommission, ohne die Einbindung demokratisch legitimierter

281 *Institutionen, erheblichen Ermächtigungsspielraum bei der Ausgestaltung*
282 *der Verordnung einräumt?*

283 Diese Durchführungsrechtsakte und delegierten Rechtsakte, die sich die
284 Kommission mit dem Entwurf selbst verschaffen würde, sind sehr kritisch
285 zu bewerten, da sie eine undemokratische Vorgehensweise darstellen.
286 Soweit möglich, sollten diese Rechtsakte schon in der Verordnung erfasst
287 werden – oder, wo nicht möglich, zumindest dem Parlament überlassen
288 werden. Das Delegieren von Detailregelungen vom Gesetzgeber auf die
289 Verwaltung durch eine (Rechts)Verordnung, die sich auf eine im Gesetz
290 enthaltene Verordnungsermächtigung stützt, ist auch im deutschen Recht
291 eine zulässige und im Grundsatz bewährte Methode. Allerdings muss eine
292 Verordnungsermächtigung stets genau aufführen, was zu regeln der
293 Verwaltung überlassen wird. Außerdem muss Wesentliches immer im
294 Gesetz selbst stehen. Der EU-Entwurf enthält sehr viele
295 Verordnungsermächtigungen (siehe Art. 86), die auch die materiellen
296 Voraussetzungen des Datenschutzes betreffen (vgl. etwa Art. 6 Abs. 5:
297 Konkretisierung des „berechtigten Interesses“; Art. 8 Abs. 3: Bestimmung
298 der Art und Weise der Einverständniserklärung). Die Kommission kann
299 hier in großem Umfang Weichenstellungen alleine vornehmen, die für die
300 praktische Anwendung entscheidend sind. Allerdings ist ein (ziemlich eng
301 befristetes) Einspruchsrecht des Parlaments vorgesehen (Art. 86 Abs. 5).
302 Das ist gut, ersetzt aber nicht das eigene Ausgestaltungsrecht des
303 Parlaments. Befremdlich erscheint auch, dass das Parlament zwar
304 Verordnungsermächtigungen aufheben kann, die bis dahin aber auf dieser
305 Grundlage erlassene Rechtsakte aber gleichwohl in Kraft bleiben (Art. 86
306 Abs. 4).

307 *23. Wie beurteilen Sie die Nichtdifferenzierung zwischen behördlichen*
308 *Datenschutzbeauftragter und Datenschutzbeauftragter*
309 *privatwirtschaftlicher Unternehmen?*

310 k.a

311 *24. Wie beurteilen Sie das Spannungsfeld zwischen dem Anspruch auf*
312 *Datenportabilität und das im Kommissionsvorschlag enthaltene „Recht auf*
313 *Vergessen“? Unterbreitet die Kommission in diesem Zusammenhang*
314 *angemessene Lösungsansätze?*

315 Das Recht auf Datenportabilität wie in Art. 18 des Kommissionsentwurf
316 spezifiziert meint die selbst eingestellten Daten in Services oder Soziale
317 Netzwerke. Damit sind der „Mehrwert“, den diese Daten für die
318 datenverarbeitende Stelle produzieren, oder etwa die Algorithmen,
319 aufgrund derer diese Daten verarbeitet werden, ausgenommen. Deshalb
320 kann dieses Recht auch nicht etwaige Betriebsgeheimnisse betreffen,
321 auch wenn dies von interessierter Seite behauptet wird. Das Recht auf
322 Vergessen, das im Berichtsentwurf des LIBE-Berichterstatteres Jan
323 Philipp Albrecht schon zutreffender „Recht auf Löschen“ genannt wird,
324 betrifft hingegen Daten, die Dritten zugänglich gemacht wurden – hier ist
325 kein Spannungsverhältnis zu erkennen. Wer seine Daten portieren will,
326 kann diese danach auch löschen lassen – sie sind dann wieder in eigener
327 Hand. Nach dem Löschen ist rein logisch ein Anspruch auf Portabilität
328 verfallen. Daten, die in einem Dienst dann Dritten zugänglich gemacht
329 worden sind, müssen auch bei diesen Dritten von der verarbeitenden
330 Stelle gelöscht werden.

331 Das Recht auf Portabilität ist eine sehr große Innovation im Bereich des
332 Datenschutzes und muss unbedingt gestärkt werden – etwa durch die
333 verbindliche Einführung von offenen Schnittstellen und offenen Formaten.

334 *25. Inwieweit beurteilen Sie das Datenschutzniveau der Grundverordnung*
335 *in Bezug auf die Widerspruchs- und Auskunftsrechte der Verbraucher*
336 *(bezgl. der über sie erhobenen Daten) als ausreichend?*

337 Die in Art. 14 und 15 vorgeschlagenen Regelungen sind umfangreich und
338 verbraucherfreundlich. Allerdings muss die Datenverarbeitung aufgrund
339 des „legitimen Interesses“ (Art. 6, Abs. 1, Satz f) erheblich eingeschränkt

340 oder am besten gelöscht werden, da hier kein Widerspruch möglich ist.
341 Durch den Grundsatz „privacy by design“ und „privacy by default“ (Art. 23)
342 sollte zudem klar sein, dass die – gerade im Zusammenhang mit dem
343 bundesdeutschen Meldegesetz diskutierte – Einwilligungslösung (Opt-in)
344 zum Standard wird.

345 Die Auskunftsrechte der Verbraucherinnen und Verbraucher sollten
346 außerdem durch eine angemessene Frist, innerhalb der die Auskunft
347 erteilt werden muss, gestärkt werden.

348 *26. Sorgt die Grundverordnung für ein angemessenes Datenschutzniveau*
349 *hinsichtlich absehbarer technologischer Entwicklungen wie beispielsweise*
350 *„SmartMeter“?*

351 Das Datenschutzniveau für absehbare technologische Entwicklungen will
352 die Kommission in der Datenschutzverordnung durch eine technologie-
353 neutrale Formulierung erreichen, worin sie stringent vorgeht. Um auch
354 absehbare technologische Entwicklungen zu erfassen, braucht es eine
355 starke Definition von personenbeziehbaren Daten in Artikel 4. Diese muss
356 deshalb unbedingt durch das Konzept der eindeutigen Bestimmbarkeit
357 statt der bloßen Identifizierbarkeit erweitert werden. Um Datenschutz zu
358 gewährleisten spielt häufig nicht so sehr die Identität aufgrund des
359 Namens der betroffenen Person eine Rolle, sondern vielmehr ihre
360 Bestimmbarkeit und Wiedererkennung aufgrund anderer Merkmale. Erst
361 wenn diese Regelung mit aufgenommen wird, ist hier ein angemessenes
362 Datenschutzniveau gewährleistet.