

1 **Antragstitel: Arbeitnehmerdatenschutz**

2
3 **Antragsteller: Landesvorstand**

4
5 Der Landesparteitag möge beschließen:

6
7 **1. Einleitung**

8
9 Die Debatte um Datenschutz und Datensicherheit hat Konjunktur. Obgleich die aktuellen
10 parlamentarischen Verfahren allenfalls als erste Schritte in die richtige Richtung gewer-
11 tet werden können, bewegt sich endlich etwas in der deutschen Datenschutzlandschaft.
12 Die Etablierung eines Datenschutzauditsiegels, die gesetzliche Normierung der OptIn-
13 Lösung oder die Beschränkung der Zulässigkeit sog. Scoringverfahren seien hierfür
14 exemplarisch genannt.

15
16 Der Arbeitnehmerdatenschutz hingegen sieht sich in diesem Zusammenhang einer ge-
17 radezu stiefmütterlichen Behandlung ausgesetzt; obgleich der Deutsche Bundestag die
18 Bundesregierung mehrfach aufgefordert hat, den Schutz von Arbeitnehmerdaten zu
19 verbessern und hierzu fraktionsübergreifende Entschlüsse vorgelegt hat, hat es
20 gesetzgeberische Aktivitäten bislang nicht gegeben.

21
22 Dabei liegt die Notwendigkeit der Schaffung klarer Strukturen für diesen Bereich auf der
23 Hand: Gerade während eines Beschäftigungsverhältnisses sammeln sich umfangreiche
24 personenbezogene Daten der Mitarbeiterinnen und Mitarbeiter an, deren Verarbeitung
25 in ganz überwiegendem Maße in automatisierter Form erfolgt. Dies gilt sowohl für privat-
26 rechtliche Anstellungsverhältnisse als auch für Beschäftigungsverhältnisse im öffentli-
27 chen Dienst.

28
29 Zudem haben nicht zuletzt die jüngsten Vorfälle im Einzelhandel gezeigt, dass die ver-
30 deckte Überwachung am Arbeitsplatz mittels Videotechnik nicht auf einzelne Fälle be-
31 schränkt bleibt. Die Bewertung dieser Sachverhalte anhand der geltenden landes- und
32 bundesdatenschutzrechtlichen Vorschriften erweist sich dabei oftmals als schwierig und
33 unübersichtlich. Sowohl Arbeitgeber als auch Arbeitnehmer werden auf eine Analyse
34 der bestehenden Rechtsprechung verwiesen, die indes regelmäßig einzelfallbezogen ist
35 und allenfalls nur von einem kleinen Expertenkreis überblickt wird.

36
37 Zwischen Arbeitnehmern und Arbeitgebern besteht oftmals kein gleichberechtigtes Ver-
38 hältnis. Arbeitnehmer machen nicht selten wegen der mangelnden Kenntnis der Rechts-
39 lage von den ihnen bereits jetzt bei Verstößen gegen datenschutzrechtliche Bestim-
40 mungen zur Verfügung stehenden Möglichkeiten keinen Gebrauch. Darüber hinaus
41 droht die Situation einzutreten, dass Arbeitnehmer aus Angst vor Repressionen oder gar
42 dem Verlust des Arbeitsplatzes auf die Geltendmachung eigener Rechte bewusst ver-
43 zichten.

44
45 Die Ausgestaltung der Rahmenbedingungen gerade eines so vielgestaltigen Themenbe-
46 reiches der Judikatur zu überlassen, erscheint als der falsche Weg. Arbeitnehmerdaten-
47 schutz ist nicht Sache des Bundesarbeitsgerichts, sondern allein des Gesetzgebers. Ein
48 gesetzgeberisches Handeln ist insoweit längst überfällig. Nur ein umfassendes Arbeit-
49 nehmerdatenschutzrecht wird dem Schutz der Persönlichkeitsrechte der Arbeitnehmer
50 gerecht.

51
52 Die Vorgabe, die datenschutzrechtlichen Belange der Arbeitnehmer und der Beschäftig-
53 ten im öffentlichen Dienst zu stärken und transparenter auszugestalten, hat sich die
54 Arbeitsgemeinschaft Arbeitnehmerdatenschutz zum Ziel gesetzt. Eingesetzt vom Lan-
55 desvorstand der FDP in Nordrhein-Westfalen wirkten hieran unter dem Vorsitz von Gi-
56 sela Piltz die folgenden Personen mit: Marco Biewald, Karl-Peter Brendel, Prof. Peter
57 Gola, Dr. Dr. h.c. Burkhard Hirsch, Dr. Joachim Jacob, Andreas Jaspers, Alexander May
58 LL.M., Dr. Robert Orth, Jan Schiller und Dr. Matthias Schulenberg.

1 Im Rahmen der Arbeitsgemeinschaft wurden insbesondere die einzelnen Abschnitte des
2 Beschäftigungsverhältnisses auf ihre datenschutzrechtliche Relevanz hin untersucht
3 und die nachfolgenden Punkte für verbesserte Regelungen erarbeitet. Die erarbeiteten
4 Grundsätze sollen vorbehaltlich besonderer beamtenrechtlicher Bestimmungen, auch
5 für Beamte und Angestellte des öffentlichen Dienstes gelten. Soweit keine besonderen
6 Bestimmungen für den Arbeitnehmerdatenschutz getroffen werden, gelten die Bestim-
7 mungen des BDSG und des BetrVG. Die vorgelegten Eckpunkte sollen nunmehr als
8 Arbeitsgrundlage für eine breite Diskussion mit weiteren Experten und Verbänden die-
9 nen. Der Landesvorstand wird beauftragt, im Nachgang die hierbei gewonnenen Er-
10 kenntnisse auszuwerten.

11 **2. Liberale Thesen**

12 **2.1. Bewerbung / Einstellung**

13 **• Grundsätzliches**

- 14 ✓ Die Daten müssen grundsätzlich beim Betroffenen erhoben werden.
- 15
- 16 ✓ Hinsichtlich der zulässigen Fragen an Bewerber ist die geltende Rechtslage
17 ausreichend. Sie sollte aber kodifiziert werden. Unzulässige Fragen dürfen we-
18 der dokumentiert noch gegenüber den Betroffenen oder Dritten durch den po-
19 tentiellen Arbeitgeber verwendet werden.
- 20
- 21 ✓ Öffentlich zugängliche Daten über den Bewerber können zur Kenntnis genom-
22 men werden (Erlangung von Spezialkenntnissen durch Nutzung von Angebo-
23 ten, die einer Registrierung bedürfen, wie z.B. XING).
- 24
- 25 ✓ Das Verbot der automatisierten Einzelentscheidung (bisher § 6a BDSG), das
26 insbesondere bei psychologischen Auswahltests eine Rolle spielen kann, soll im
27 Arbeitsrecht eindeutig festgeschrieben werden.
- 28

29 **• Einstellungs- und weitere Untersuchungen**

- 30 ✓ Untersuchungen, die keine Aussage zur Leistungsfähigkeit des Arbeitnehmers
31 bzgl. der konkreten Tätigkeit zulassen, dürfen nicht vorgenommen werden.
- 32
- 33 ✓ Gentests oder Fragen zu genetischen Dispositionen sollen grundsätzlich aus-
34 geschlossen werden.
- 35
- 36 ✓ Bei gefahrgeneigter Tätigkeit soll es zum Schutz Dritter, des Arbeitgebers und
37 des Arbeitnehmers selbst möglich sein, regelmäßige Untersuchungen durch-
38 zuführen. Diese Untersuchungen sollen allerdings nur möglich sein, wenn sie
39 für die Eignung der Tätigkeit zwingend notwendig sind (z.B. Alkoholtest bei Lkw-
40 Fahrer).
- 41

42 **2.2. Das laufende Beschäftigungsverhältnis**

43 **• Umgang mit Bewerbungsunterlagen**

- 44 ✓ Bewerbungsunterlagen sind dem Bewerber zurückzusenden und die Bewerber-
45 daten zu löschen. Im Falle einer erfolglosen Bewerbung dürfen Daten nur so
46 lange aufbewahrt werden, wie dies rechtlich geboten ist, z.B. im Hinblick auf
47 das Allgemeine Gleichbehandlungsgesetz (AGG). Wird eine längere Aufbewah-
48 rung seitens des Arbeitgebers gewünscht, setzt dies das Einverständnis des
49 Bewerbers voraus.
- 50

51 **• Personalakte**

- 1 ✓ Zur Personalakte gehören alle Unterlagen und Vorgänge, die in einem unmittelbaren inneren Zusammenhang mit dem Beschäftigungsverhältnis des Mitarbeiters stehen. Zur Personalakte gehören daher auch alle schriftlichen Aufzeichnungen, die sich mit der Person des Arbeitnehmers und dem Inhalt und Verlauf seines Beschäftigungsverhältnisses befassen. Es ist dabei nicht entscheidend, wo, in welcher Form und unter welcher Bezeichnung die Daten gespeichert sind.
- 2
3
4
5
6
7
8
- 9 ✓ Wer Personalentscheidungen zu treffen hat, dem stehen die für eine sachgerechte Entscheidung erforderlichen Unterlagen zur Verfügung. Der Kreis der Zugriffsberechtigten ist möglichst klein zu halten. Bei elektronischer Aktenführung muss die Zugriffsberechtigung geregelt werden. Betriebsräte haben nur mit Zustimmung des Betroffenen Einsicht in die Personalakte. Auf Stammdaten können der Dienstvorgesetzte und der Betriebsrat zugreifen.
- 10
11
12
13
14
15
- 16 ✓ In die Personalakte dürfen nur konkrete korrekte Informationen/Daten aufgenommen werden. Andernfalls stehen dem Betroffenen gegen die entsprechenden Inhalte/Daten unabhängig von der Art der Verarbeitung neben dem bestehenden arbeitsrechtlichen Recht der Gegendarstellung Abwehrrechte nach dem BDSG (Löschung, Berichtigung, Auskunft, Sperrung) zur Verfügung.
- 17
18
19
20
21
22

23 • **Weitergabe von Arbeitnehmerdaten an Dritte**

- 24
- 25 ✓ Die Übermittlung von Arbeitnehmerdaten an Dritte ist ohne Einwilligung des betroffenen Mitarbeiters nur dann zulässig, wenn ein „gravierendes Interesse“ an der Durchbrechung des Grundsatzes der Vertraulichkeit besteht. Ein solches gravierendes Interesse kann z.B. bei Unternehmensverkäufen bestehen.
- 26
27
28
29
- 30 ✓ Bei einem Unternehmensverkauf mit „Due Diligence Prüfungen“ dürfen Daten nur anonymisiert weitergegeben werden. Daten von Angestellten i.S.v. § 5 Abs. 2 bis 4 BetrVG dürfen jedoch weiter gegeben werden.
- 31
32
33
- 34 ✓ Ein europaweites Konzernprivileg ist grundsätzlich möglich. Über Europa hinaus soll ein Konzernprivileg nur dann möglich sein, wenn ein vergleichbares Datenschutzniveau besteht und die Rechte des Betriebsrates – nämlich die Einhaltung der gesetzlichen Voraussetzungen zu prüfen – erhalten bleiben.
- 35
36
37
38

39 • **Whistleblowing**

- 40
- 41 ✓ Für das so genannte Whistleblowing sind keine besonderen Regelungen notwendig. Die allgemeinen Grundsätze und Regelungen (§ 241 BGB – allgemeine Pflichten aus dem Schuldverhältnis) sind dafür ausreichend.
- 42
43
44

45 • **Zugangskontrollen und biometrische Daten**

- 46
- 47 ✓ Biometrische Daten dürfen nur zu dem Zweck verwendet werden, für den sie ursprünglich erhoben wurden. Zweckänderungen sind unzulässig.
- 48
49
- 50 ✓ Zugangskontrollen sollen grundsätzlich nur der Identitäts- und Anwesenheitskontrolle dienen.
- 51
52
- 53 ✓ Die Arbeitnehmer müssen darüber informiert werden, welche Daten gespeichert werden.
- 54
55
- 56 ✓ Lösungen, bei denen die gespeicherten Referenzdaten unter der alleinigen Kontrolle der Betroffenen stehen und ausschließlich zum Vergleich verarbeitet werden (datensparsame Templates), sind vorzuziehen.
- 57
58
59

- 1 ✓ Nichtdiskriminierende Ausweichmöglichkeiten sind grundsätzlich vorzusehen,
2 da ein ausnahmsloser Benutzerzwang gegen das Recht auf informationelle
3 Selbstbestimmung verstoßen kann.
4
5 ✓ Insbesondere lassen sich grundsätzlich biometrische Verfahren, die der Verifi-
6 kation dienen, mit einer dezentralen Datenspeicherung betreiben (1:1 Abgleich).
7
8 ✓ Es müssen detaillierte Zugriffskonzepte geschaffen werden, um eine zweckwid-
9 rige Nutzung zu vermeiden und die Daten vor unberechtigtem Zugriff und vor
10 Diebstahl zu schützen.
11
12 ✓ Eine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten ist zu e-
13 tablieren.
14
15 ✓ Biometrische Daten sollen innerhalb festgesetzter Fristen gelöscht werden. Die
16 Löschung muss überprüfbar sein.

17
18 • **Arbeitnehmerüberwachung per Video und permanente Systeme zur Überwa-**
19 **chung der Leistungsfähigkeit**

- 20
21 ✓ Heimliche Videoüberwachungen sind grundsätzlich nicht gestattet.
22
23 ✓ Neben dem im Einzelfall berechtigten Einsatz spezieller Überwachungssysteme
24 dürfen Videoüberwachungssysteme oder andere permanente technische Sys-
25 teme mit vergleichbarer Eingriffsintensität (RFID, GPS) nicht zu Zwecken der
26 Leistungs- und Verhaltenskontrolle, zum Leistungsvergleich oder zur Leistungs-
27 bemessung eingesetzt werden. Dies gilt insbesondere für Verfahren des Data-
28 minings oder Screenings.
29
30 ✓ Die Überwachung von Produktionsabläufen zur Einhaltung gewerblicher Aufla-
31 gen sowie von Kassen und sonstigen öffentlich zugänglichen Geschäftsberei-
32 chen soll möglich bleiben.
33
34 ✓ Vor dem Einsatz von Videoüberwachung oder anderen permanenten techni-
35 schen Systemen mit vergleichbarer Eingriffsintensität ist eine Vorabkontrolle
36 des Systems durch den betrieblichen Datenschutzbeauftragten durchzuführen.
37
38 ✓ Die Überwachung von einzelnen Beschäftigten mittels Videoüberwachung und
39 Aufzeichnungssystemen oder anderen permanenten technischen Systemen mit
40 vergleichbarer Eingriffsintensität ist grundsätzlich untersagt, ebenso wie Video-
41 überwachung, die die Intimsphäre der Arbeitnehmer verletzt (z.B. Toilette und
42 Umkleidekabinen).
43
44 ✓ Auswertungen von Videoaufzeichnungen oder anderen permanenten techni-
45 schen Systemen mit vergleichbarer Eingriffsintensität dürfen bei konkretem An-
46 lass zur Aufklärung oder Verhinderung von Straftaten genutzt werden und sind
47 zu protokollieren.
48
49 ✓ Aufzeichnungen sind unverzüglich zu löschen, wenn sie nicht mehr erforderlich
50 sind oder schutzwürdige Interessen der Beschäftigten entgegenstehen.
51
52 ✓ Unzulässige Videoaufzeichnungen oder Dokumentationen anderer permanenter
53 technischer Systeme mit vergleichbarer Eingriffsintensität dürfen nicht gegen
54 den Betroffenen verwendet werden.
55

56 • **Überwachung von Internet-, Email- und Telefonnutzung (Informations und Kom-**
57 **munikationstechnik)**
58

- 1 ✓ Auch bei dienstlicher Nutzung von z.B. E-Mail, Internet oder Telefon ist eine
2 Auswertung, die die systematische Kontrolle des Beschäftigten zum Ziel hat,
3 unzulässig.
4
- 5 ✓ Möglich sind daneben lediglich stichprobenhafte und zeitnahe Auswertungen zu
6 Protokolldaten. Dabei ist ein transparentes Verfahren sicher zu stellen.
7
- 8 ✓ Straf- und Ordnungswidrigkeitsvorschriften sind entsprechend anzupassen.
9
- 10 ✓ Die Arbeitnehmer sind über die Inhalte und Details von Protokolldaten zu infor-
11 mieren. Lösungsfristen sind vorzusehen.
12
- 13 ✓ Eine technische Überwachung des digitalen Arbeitsplatzes ohne Kenntnis der
14 Arbeitnehmer darf grundsätzlich nicht durchgeführt werden.
15
- 16 ✓ Der Arbeitgeber ist nicht verpflichtet, die private Nutzung von E-Mails, Internet
17 und Telefon zu gestatten oder als sozialadäquates Verhalten zu dulden.
18
- 19 ✓ Soweit der Arbeitgeber die private Nutzung von Informations- und Kommunika-
20 tionstechnik gestattet, hat er für den Schutz der Privatsphäre des Arbeitneh-
21 mers Sorge zu tragen.
22
- 23 ✓ Eine flächendeckender Abgleich von Emailkommunikationsdaten widerspricht
24 dem Grundsatz der Verhältnismäßigkeit und ist grundsätzlich ausgeschlossen.
25 Organisatorische Maßnahmen, wie z.B. die Formulierung von Verhaltenskodi-
26 zes, sind vorzuziehen. Nur im Einzelfall kann ein erheblich überwiegendes Inter-
27 resses des Arbeitgebers gegeben sein, eine Auswertung der Emailkorrespon-
28 denz des Arbeitnehmers vorzunehmen. Denkbar sind hierbei konkrete sich ver-
29 dichtende Verdachtsmomente, die auf die Begehung einer nicht nur unerhebli-
30 chen Pflichtverletzung des Arbeitnehmers hinweisen, z.B. Verdacht auf Korrup-
31 tion. Der Betriebsrat ist in etwaige Ermittlungsmaßnahmen einzubeziehen. Die
32 Betroffenen sind im Nachhinein über den erfolgten Abgleich zu informieren.
33

34 2.3. Arbeitnehmerdatenschutz und betriebliche Mitbestimmung

- 35
- 36 ✓ Der Betriebsrat muss datenschutzrechtliche Belange der Arbeitnehmerinnen
37 und Arbeitnehmer wahrnehmen können. Dies gilt insbesondere vor dem Hinter-
38 grund des bestehenden Abhängigkeitsverhältnisses zwischen Arbeitnehmer
39 und Arbeitgeber, das nicht zu einer „datenschutzrechtlichen Abhängigkeit“ des
40 Arbeitnehmers führen darf, z.B. diesen zur Zustimmung zu Erhebung, Nutzung
41 und Verarbeitung von Daten zu bewegen.
42
- 43 ✓ Die Mitbestimmungsregeln zugunsten des Betriebsrates dürfen nicht dazu füh-
44 ren, dass der einzelne Arbeitnehmer übergangen wird, z.B. wenn es um die Zu-
45 stimmung zu Überwachungsmaßnahmen geht. Das Allgemeine Persönlichkeits-
46 recht ist ein höchstpersönliches Rechtsgut und darf nicht der alleinigen Disposi-
47 tion eines Kollektivorgans unterworfen werden.
48
- 49 ✓ Eine Informationspflicht des Arbeitgebers gegenüber den Betriebsräten im Hin-
50 blick auf Arbeitnehmerdatenverarbeitung außerhalb der Personalverwaltung ist
51 zu etablieren.
52
- 53 ✓ Die Beachtung datenschutzrechtlicher Bestimmungen und die Sanktionierung
54 von etwaigen Verstößen muss auch in Betrieben sichergestellt werden, die nicht
55 über einen Betriebsrat verfügen. An die Verletzung der Unterrichtungspflicht an
56 den betrieblichen Datenschutzbeauftragten muss eine unmittelbare Rechtsfolge
57 geknüpft sein.
58

- 1 ✓ Transparenz im Mitbestimmungsrecht soll gefördert werden, wobei eine unnöti-
2 ge Behinderung des Produktivgeschäftes vermieden werden sollte.
- 3
- 4 ✓ Eine Informationspflicht für den Fall der Datenverarbeitung im Auftrag, auch im
5 Bereich der Personalverwaltung, ist zu etablieren.
- 6

7 **2.4. Umgang mit Daten des Arbeitnehmers nach Beendigung**
8 **des Beschäftigungsverhältnisses**

- 9
- 10 ✓ Soweit Daten der Arbeitnehmer nicht mehr zur Sicherung von Rechtspositionen
11 benötigt werden, sind diese umgehend und umfassend zu löschen.
- 12
- 13 ✓ Dem ausgeschiedenen Arbeitnehmer muss die Möglichkeit eröffnet werden,
14 den Löschvorgang einzusehen und nachvollziehen zu können.
- 15
- 16 ✓ Soweit gesetzliche oder vertragliche Vorgaben eine umgehende Löschung ver-
17 bieten, sind die verbleibenden Daten nur für diese konkreten Vorgaben zu ver-
18 wenden. Eine anderweitige Nutzung ist ausgeschlossen.
- 19
- 20 ✓ Nach Ablauf der Aufbewahrungsfristen sind vorhandene Unterlagen einer ord-
21 nungsgemäßen Entsorgung (nach DIN 32757 Stufe 3) zuzuführen. Die Entsor-
22 gung ist zu dokumentieren.
- 23
- 24 ✓ Die Verarbeitung gesperrter personenbezogener Daten ist grundsätzlich unter-
25 sagt.
- 26

27
28 **Begründung:**

29
30 erfolgt mündlich

31
32

33
34 **BESCHLUSS:**

35