DIGITALE NUTZERRECHTE

SCHWERPUNKT DATENSCHUTZ

August 2014

AK ÖSTERREICH

GERECHTIGKEIT MUSS SEIN

Bundesarbeitskammer Positionspapier Datenschutz-Grundverordnung und Konsumentenschutz

Regelungsdefizite im und Lösungsansätze für den Entwurf zu einer Datenschutz-Grundverordnung im Detail

1. **Anonymisierungsgebot:** In Fällen, wo die Notwendigkeit eines Personenbezugs nicht nachgewiesen ist, müssen Daten restlos anonymisiert werden. Das Prinzip der Datensparsamkeit gebietet diese Vorgangsweise. Dies muss in der Verordnung auch klar zum Ausdruck kommen. Benötigt wird ein Verbot, dass „wenn der Zweck der Verarbeitung es nicht erfordert, der Auftraggeber keine Identifizierung vornehmen darf."

2. **Pseudonymisierung als Ausnahmefall:** Als „pseudonymisierte Daten" gelten personenbezogene Daten, die einer Person ohne zusätzliche Informationen nicht eindeutig zugeordnet werden können. Derartige Zusatzinformationen sind getrennt aufzubewahren und ihre Zuordnung zu einer konkreten Person muss durch technische bzw. organisatorische Maßnahmen unterbunden werden. Oft werden anonymisierte und pseudonymisierte Daten in einem Atemzug unterschiedslos genannt. Während aber erstere keinerlei Personenbezug aufweisen und für den Datennutzer auch ein solcher nicht mehr herstellbar ist, gilt für letztere Datenkategorie das Gegenteil: dem Datenverwender ist es jederzeit möglich, einen Personenbezug - unter Abgehen von der allenfalls getroffenen Übereinkunft, keine Identifizierung vorzunehmen – wieder herzustellen. Für eine Pseudonymisierung gibt es einige zweckmäßige Anwendungsgebiete (zB bei der Anmeldung von KonsumentInnen bei Internetforen oder sozialen Netzwerken mit der Vereinbarung, dass in speziell geregelten Fällen – wie etwa strafrechtlichen Verstößen des Dienstenutzers – die Pseudonymisierung vom Diensteanbieter aufgehoben und die echten Stammdaten an die zuständigen Behörden weitergegeben werden können). Auch Zeitverlaufs-Studien greifen oft auf pseudonymisierte Daten zurück, um neue Sachverhalte einer individuellen Person im Zeitverlauf zuordnen zu können.

   Rechtliche Erleichterungen für die Verwender pseudonymisierter Daten sind aber in der Regel unangebracht. Aus Datenschutzsicht erweckt Pseudonymisierung oft den Eindruck einer Pseudolösung. Denn in der Praxis ist eine vollständige Anonymisierung häufig möglich und rechtlich geboten. Im Wege einer reinen Pseudonymisierung kann sich der Datenverwender hingegen alle Möglichkeiten einer personenbezogenen Nutzung (etwa im Wege der Änderung seiner Geschäftsklauseln) auf Dauer offenhalten. Pseudonymisierungszusagen eröffnen auch schwer kontrollierbare Missbrauchspotentiale.

3. **Gesamtverantwortung des Auftraggebers einer Datenverarbeitung:** Die EU-Kommission hatte die Klarstellung vorgeschlagen, dass personenbezogene Daten „unter der Gesamtverantwortung des für die Verarbeitung Verantwortlichen“ verarbeitet werden, der dafür haftet, „dass bei jedem Verarbeitungsvorgang die Vorschriften dieser Verordnung eingehalten werden, und der den Nachweis hierfür erbringen muss.“ Ein expliziter Hinweis auf die Gesamtverantwortung und Beweispflichten ist notwendig. Damit kann verhindert werden, dass Datennutzer ihre Verantwortung im Konfliktfall auf untergeordnete Datenverantwortliche und Dienstleister abzuwälzen versuchen.

4. **Höhere Anforderungen an die Zustimmung zur Datennutzung:** Eine verbraucherpolitisch zentrale Maßnahme ist, dass die Zustimmung der Betroffenen zur Nutzung ihrer personenbezogenen Daten künftig ausdrücklich erfolgen muss. Diese Änderung bedeutet eine deutliche Anhebung des bisherigen Datenschutzniveaus. Eine Zustimmung durch stillschweigende Akzeptanz von Geschäftsbedingungen darf nicht mehr möglich sein. Für eine wirksame Einwilligung muss sich der Datennutzer jedenfalls um ein aktives Zeichen der KonsumentInnen bemühen. Realisiert werden kann dies durch Setzen eines Hakens beim Anklicken eines Kästchens im Internet oder Einholen der Unterschrift. Zustimmungserklärungen dürfen auch nicht mehr in Geschäftsbedingungen versteckt werden. Die Einwilligung muss erkennbar und von anderen Texten getrennt sein. Versuchen, diese Anforderungen wieder aufzuweichen, ist eine Absage zu erteilen. So ist eine „unzweifelhafte“ zB nicht einer „ausdrücklichen“ Zustimmung gleichzuhalten.

5. **Mehr Schutz vor Direktmarketing**: Viele KonsumentInnen fühlen sich durch Direktwerbung in hohem Maß belästigt. Viele der im Internet gewählten Tracking-Methoden, ein Verhaltensprofil der Internetnutzer für Werbezwecke anzulegen sind intransparent und oft auch rechtswidrig. Die Anforderungen an das Direktmarketing sollten unbedingt verschärft und eine Zustimmungspflicht zur Datennutzung auch in diesem Bereich eingeführt werden. Eine Privilegierung des Direktmarketings durch eine bloße Opt-Out-Regel, bei der Verbraucher gegen die Verwendung ihrer Kundendaten zu Werbezwecken nur ein Widerrufsrecht zusteht, ist nicht sachgerecht. Sämtliche datenschutzbezogenen Lippenbekenntnisse, Datenschutz im Internet verbessern zu wollen, verlieren an Glaubwürdigkeit, wenn Direktwerbeunternehmen, also etwa Google, das Privileg genießen, sich über die Souveränität der Internetnutzer in Bezug auf ihre Daten hinwegsetzen und Daten ohne Zustimmung für Werbezwecke nutzen können. Erschwerend kommt hinzu, dass nicht einmal die Datenarten geregelt sind, die von diesem Nutzungsprivileg erfasst sind.

Eine Opt-Out Regelung für Direktwerbung ist völlig unakzeptabel, da damit auch das Versprechen nach einem zeitgemäßen Datenschutz im Internet nicht ansatzweise eingelöst würde.

6. **Keine „unfreiwilligen" Zustimmungen:** Einwilligungen sollen außerdem unwirksam sein, wenn zwischen den Positionen des Betroffenen und des Datenverarbeiters ein klares Ungleichgewicht besteht. Dazu zählen Abhängigkeiten wie sie bspw. bei Arbeitnehmerverhältnissen typisch sind. Ungleiche Kräfteverhältnisse bestehen aber auch bei Verbrauchergeschäften. Unternehmen verweigern KonsumentInnen häufig Vertragsabschlüsse, wenn diese einer Datennutzung für Marketingzwecken nicht zustimmen. Die Freiwilligkeit einer Zustimmung ist daher auch standardmäßig anzuzweifeln, wenn Verbraucher, die einer Datennutzung nicht zustimmen in der Folge vom Bezug der Ware oder Dienstleistung ausgeschlossen werden (Koppelungsangebote) und keine Alternativangebote am Markt finden.

7. **Klare Ge- und Verbote statt unbestimmter Erlaubnistatbestände:** Die Datennutzung soll nach dem Wunsch von Kommission, Parlament und Rat auch „im überwiegenden berechtigten Interesse" des Auftraggebers (oder Empfängers) erfolgen können. Dieser Regelungsansatz ist unbestimmt, bietet wenig Rechtssicherheit und kann auch unvertretbar weit ausgelegt werden. Deshalb sind die Datennutzungen anzuführen, bei denen typischerweise von einem solchen überwiegenden Interesse auszugehen ist. Ebenso sind Fälle zu benennen, wo dies ausgeschlossen wird.

8. **Datennutzung nur im Rahmen des Ursprungszweckes:** Es sollte unbedingt auch darauf hingewiesen werden, dass Daten nicht für Zwecke genutzt werden dürfen, die mit dem originären Speicherzweck nicht in Einklang stehen. Ausnahmen von diesem Verbot (wie die Verarbeitung für statistische oder historische Zwecke) sind restriktiv zu handhaben und taxativ anzuführen. Wer Daten über den ursprünglichen Zweck hinaus für andere Sekundärzwecke nutzen möchte, benötigt dafür eine eigene Rechtsbasis (zB die Zustimmung der Betroffenen). Der Regelungstechnik eines allgemeinen Weiterverarbeitungsverbots für andere Zwecke plus weniger begründeter Ausnahmen ist der Vorzug zu geben. Vage Kriterien, die bei der Abwägung unterstützen sollen, werden abgelehnt.

9. **Ausdehnung des EU-Datenschutzes auf Drittländer:** Die Anwendbarkeit der künftigen Datenschutz-Verordnung auf Anbieter aus Drittländern, zB Internetdienste von US-Anbietern, auszudehnen, ist dringend erforderlich. Der EU-Datenschutzstandard soll greifen, wenn Daten über KonsumentInnen innerhalb der EU von einem Unternehmen, das nicht innerhalb der EU niedergelassen ist, gesammelt werden.

Voraussetzung dafür ist, dass deren Datenverarbeitung dazu dient, europäischen Verbrauchern Waren oder Dienste anzubieten oder ihr (Nutzungs-)Verhalten zu beobachten. Die Einbeziehung ist bedeutsam, da vielen Internetangeboten von großer Reichweite und datenschutzrechtlicher Brisanz oft keine europäische Niederlassung zurechenbar ist. Gleichzeitig müssen aber auch Vollstreckungsübereinkommen mit den USA vorangetrieben werden, andernfalls werden vorhandene Rechtsansprüche europäischer Bürgerinnen weiterhin schwer durchsetzbar sein.

10. **Automatische Verbraucherinformation:** Von Verarbeitungen Betroffene müssen vor der Datenermittlung mehr Informationen vom Datennutzer erhalten. KonsumentInnen muss bei der Datenerhebung bzw innerhalb einer angemessenen Frist u.a mitgeteilt werden: neben dem Namen und den Kontaktdaten des Datenverantwortlichen, die Nutzungszwecke, erstmals auch die konkrete Speicherdauer, die Herkunft der Daten, ob die Bereitstellung der Daten verpflichtend oder freiwillig ist uä. Diese Maßnahme dient der Transparenz und ist die unbedingte Voraussetzung dafür, dass KonsumentInnen ihre Rechte in der Praxis wahrnehmen können. Ohne Kenntnisse, wer, welche Daten, wozu verarbeitet, können Betroffene auch von ihren Auskunfts-, Widerrufs-, Löschungs- und Berichtigungsrechten nicht gezielt Gebrauch machen. Diese Informationen dürfen nur entfallen, wenn die Realisierung unmöglich ist - nicht aber auch, soweit sie mit einem „unverhältnismäßig hohen Aufwand“ verbunden ist. Diese Einschränkung höhlt die Transparenznorm aus und führt zu hoher Rechtsunsicherheit, weil die Frage nach der Zumutbarkeit eines Aufwands – ohne unternehmensinterne Kenntnisse - weder vom Betroffenen noch von den Datenschutzbehörden verlässlich beurteilt werden kann.

11. **Lückenloses Auskunftsrecht:** Das Recht auf Auskunft muss jederzeit - zumindest einmal jährlich – und in jeder Hinsicht kostenlos ausgeübt werden können. Zeitliche Einschränkungen sind abzulehnen. Selbstverständlich müssen im Rahmen der Auskunft auch die einzelnen Datenarten angeführt werden. Alles andere würde einen massiven, nicht sachlich begründbaren Rückschritt zur geltenden Rechtslage bedeuten. Die Möglichkeit des Auskunftssuchenden, eine „Kopie“ der Daten anzufordern, ist kein gleichwertiger Ersatz: sie ist mit einer Kostenpflicht verbunden und kann verweigert werden, wenn in Textteilen Daten Dritter enthalten sind. Die Ausübung des Auskunftsrechts darf keinesfalls daran scheitern, dass nach dem Konzept des Rates nur eine „Kopie“ der Datenanwendung herauszugeben ist und die Herausgabe verweigert werden kann, wenn dritte Personen darin aufscheinen. Diesfalls muss der Auftraggeber den Dateninhalt, soweit es den Auskunftswerber betrifft, zusammengefasst wiedergeben. Ein Rückschritt gegenüber dem Status Quo ist undenkbar.

12. **Strikte Auskunftspflicht über die Datenherkunft:** Auch die Auskunftspflicht bezüglich der Herkunft von Daten bezieht sich weiterhin nur auf „verfügbare" Daten, was zur Folge hat, dass - ohne lückenlose Dokumentationspflicht - es in der Hand des Datenverantwortlichen liegt, ob er Auskünfte zur Datenquelle (vollständig) erteilt oder nicht.

13. **Strikte Auskunftspflicht über die Empfänger:** Der Auftraggeber hat derzeit über „Empfänger oder Empfängerkreise" zu informieren. Die Aussagekraft zwischen diesen beiden Kategorien kann unterschiedlicher nicht sein. Der Verpflichtung wird schon entsprochen, wenn die Branche (zB „Finanzdienstleister") offengelegt wird. Der Betroffene kann seine Rechte nur ausüben, wenn das jeweilige einzelne Unternehmen benannt wird. Folglich muss unbedingt hinzugefügt werden, dass grundsätzlich die Empfänger namhaft zu machen sind. Die Angabe bloßer Empfängerkreise reicht nur in Verbindung mit einer schlüssigen Begründung, weshalb die konkreten Empfänger ausnahmsweise nicht bekannt sind.

14. **Spezielle Löschungsrechte im Internet:** Mit Blick auf im Internet veröffentlichte Personendaten bedarf es eines Rechtsanspruchs, bspw. als Besitzer eines Facebook-Profils durch vollständige Datenlöschung auf Wunsch wieder „vergessen zu werden". Ein Fortschritt wäre auch die Verpflichtung desjenigen, der personenbezogene Daten im Internet veröffentlicht hat, „alle vertretbaren Schritte" zu setzen, Dritte, die diese Daten weiterverarbeiten, darüber zu informieren, dass der Internetnutzer die Löschung aller Querverweise und Kopien verlangt hat. Der Entwurf regt auch zu datenschutzfreundlichen Voreinstellungen bei Internetdiensten. Die BAK fordert bereits in der Verordnung festzuhalten, dass von Plattformbetreiber wie sozialen Netzwerken vorgegebene Privatsphäre-Werkzeuge anbieterseits so voreinzustellen sind, dass dadurch Daten der Öffentlichkeit nicht zugänglich werden.

    Der Kommissionsentwurf enthält als eine der zentralen Verbesserungen zum Status Quo auch „Rechte gegenüber Empfängern". Es ist zeitgemäß und wichtig, Betroffene von der Last zu befreien, eine Löschung auf allen Ebenen einer Übermittlungskette auf sich allein gestellt durchsetzen zu müssen. Es ist daher keinesfalls der Rats-Empfehlung zu folgen, von folgender Verpflichtung abzusehen: „Der für die Verarbeitung Verantwortliche muss allen Empfängern, an die Daten weitergegeben wurden, jede Berichtigung oder Löschung ….mitteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden."

15. **Strikte Löschroutinen:** Dem Kommissionsvorschlag zufolge „hat der für die Verarbeitung Verantwortliche Vorkehrungen zu treffen, um sicherzustellen, dass die Fristen für die Löschung personenbezogener Daten und/oder die regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung eingehalten werden." Damit sind elementare Sorgfaltspflichten zwar nicht präzise geregelt, aber zumindest angesprochen. Eine Eliminierung - wie vom Rat vorgeschlagen - kommt nicht in Frage.

16. **Umfangreiches Widerspruchsrecht:** Für die erfolgreiche Ausübung des Widerspruchsrechts gegen eine Datenverarbeitung sind der Bestimmung zufolge „Gründe, die sich aus einer besonderen Situation ergeben" anzuführen. Ein begründungsloses Widerspruchsrecht gibt es, offenbar nur für den Fall der Direktwerbung. Unbedingt hinzuzufügen ist, dass einmal erteilte Zustimmungen vom Betroffenen jederzeit widerrufen werden können. Auf dieses Widerrufsrecht hat der Auftraggeber den Betroffenen auch hinzuweisen. Außerdem muss Betroffenen ein begründungsloses Widerspruchsrecht zustehen. Dies ist nach geltender Rechtslage der Fall, wenn die Daten des Betroffenen in eine gesetzlich nicht angeordnete, aber öffentlich zugängliche Datenanwendung aufgenommen worden sind.

17. **Klare Grenzen für Profilbildung und Personenbewertung:** Die Vorschläge von EU-Kommission, dem EU-Parlament wie dem Rat schaffen einen breiten Erlaubnistatbestand für die an Scoring und Profiling interessierte Wirtschaft. Datenschutz und Rechtsschutzanliegen der Verbraucher kommen dabei jedenfalls zu kurz. Zunächst werden unter dem Titel „Profiling" nicht alle heiklen Datennutzungen erfasst, bei denen automatisierte Einzelentscheidungen getroffen werden. Es ist daher wichtig, dass nicht nur die Bildung von gesamten Personenprofilen sondern auch die Bewertung von bestimmten Einzelmerkmalen von Personen (zB Finanzkraft, Vorlieben, Gesundheit usw) und Verhaltensprognosen (wie zB erwartetes Zahlungsverhalten, Kaufhäufigkeit) durch Datenanalyse- und Prognoseinstrumente geregelt werden.

    Die bisher am Tisch liegenden Vorschläge erfassen die gegenwärtigen (und umso mehr noch die künftigen) Probleme mit dem unverhältnismäßigen Einsatz von Datamining – und Scoring-Methoden nicht ansatzweise. Entscheidende Fragen werden ausgeklammert: unter welchen Voraussetzungen dürfen Scorings eingesetzt und Personenprofile überhaupt gebildet werden? Welche Datenarten dürfen diesfalls maximal verarbeitet werden? Welche Anforderungen stellt man an die wissenschaftliche Aussagekraft und Haltbarkeit von Prognosewerkzeugen, damit Betroffene nicht willkürlichen und diskriminierenden Verhaltenszuschreibungen ausgesetzt sind?

Angesprochen werden immerhin die Informations- und Auskunftsrechte der Betroffenen. Mit keinem Wort erwähnt werden aber die Besonderheiten, die bei der Ausübung des Auskunftsrechtes zur berücksichtigen sind (etwa in Bezug auf die in die Gesamtbewertung der Person einfließenden Kriterien und Gewichtungen). Keinesfalls zuzustimmen ist der Einschränkung, dass die Auskunft über die Logik und die Folgen des Einsatzes einer Scoringssoftware Betroffenen nur zu erteilen ist, als Geschäfts- und Betriebsgeheimnisse der Auskunftserteilung nicht entgegenstehen. Diese vage Anordnung widerspricht dem Bedürfnis betroffener Verbraucher nach einer vollständigen, transparenten Auskunft. Die Vorschläge lassen auch offen, wann eine automatisierte Entscheidungsfindung überhaupt „notwendig" ist für den beabsichtigten Vertrag zwischen dem Auftraggeber und dem Betroffenen (es fehlen etwa Bagatellgrenzen, eine Beschreibung der Vertragstypen, Branchen etc.). Die Zulässigkeit einer Profilbildung und einer Personenbewertung darf keinesfalls nur auf der Zustimmung des Betroffenen aufbauen. Es darf nicht ernsthaft angenommen werden, dass eine solche Zustimmung des Verbrauchers in diesem Zusammenhang jemals freiwillig erfolgt.

Kurz, es fehlt an vielem. Etwa einer Auseinandersetzung mit:

- dem zulässigen Datenumfang: Zahlungsanstände; mit anderen Worten: Vorliegen von Negativdaten, keine Positivdaten „auf Vorrat", keine Daten von Direktwerbeunternehmen, keine Medieninformationen über Privatpersonen
- Bagatellgrenzen (Voraussetzung: Kreditierung, Überschreiten eines Schwellwertes)
- Ausübungsregeln für automatisierte Bewertungen (Diskriminierungsverbot, Transparenzgebot, Zertifizierung u.a.m)
- Informationspflichten vor der Datenermittlung gegenüber den Betroffenen
- einer lückenlosen Protokollierung der Datenherkunft
- einer dichten Aktualisierung des Datenbestandes
- präzisen Löschfristen
- Widerrufsrechten, soweit die Datennutzung zustimmungspflichtig ist (dazu zählt das Anlegen von Identitätsdaten ohne Zahlungsanstände)
- einer branchenfinanzierten Schlichtungsstelle

18. **Datenverarbeiter sollen mehr Eigenverantwortung übernehmen**: Die EU-Kommission möchte Datennutzer stärker in die Verantwortung nehmen – durch verpflichtende Dokumentationen, Sicherheitsmaßnahmen, Datenschutzbeauftragte (in bstimmten Fällen) und eine Risikoabschätzung bei heiklen Datenanwendungen etwabei Personenprofilen, Scoring und der Nutzung von Gesundheitsdaten. Dies ist grundsätzlich zu unterstützen. Datenschutzbehörden können nicht Millionen Datenanwendungen gleichzeitig im Auge behalten und sind derzeit auf Beschwerden angewiesen.

Viele Verarbeitungen finden ohne Wissen der KonsumentInnen „hinter den Kulissen“ statt, weshalb nicht allein auf das Einlangen von Anzeigen gesetzt werden kann.

Der EU-Kommissionsentwurf enthält gute Ansätze bezüglich der stärkeren Verantwortlichkeiten der Datenverarbeiter. Die Ausgestaltung der Vorschriften ist jedoch so mangelhaft, dass sie ohne Überarbeitung kaum Nutzen stiften. Unausgereifte Regeln über Dokumentationspflichten und Risikoanalysen sowie verpflichtende Datenschutzbeauftragte ausschließlich in Betrieben mit extrem hoher Beschäftigtenzahl schaffen keinen akzeptablen Ausgleich für einen Wegfall der Transparenz- und Kontrollbestimmungen (Meldeverfahren und zur Vorabkontrolle) nach der gegenwärtigen Rechtslage.

Deshalb braucht es noch mehr: Datenverarbeiter sollen sensible Vorhaben auf eigene Kosten durch unabhängige Begutachtungsstellen prüfen lassen müssen, damit Datenschutzkonformität im Großen und Ganzen gewährleistet ist (ob ein Vorhaben als datenschutzrechtlich „heikel“ einzustufen ist, sollten die Datenschutzbehörden entscheiden).

Auf die Eigenverantwortung des Datennutzers zu setzen, darf außerdem nicht dazu führen, dass bisherige Kontrollvorschriften wie das Meldeverfahren und die behördliche Vorabkontrolle aufgegeben werden. Das Melderegister erfüllt einen Publizitätszweck (Verbraucher können Einsicht nehmen) und hilft der Datenschutzbehörde, einen Überblick über die Verarbeitungspraxis zu erhalten. Angesichts der schieren Menge an Meldungen (und leider auch rechtswidrig unterlassenen Registrierungen) kann die Datenschutzbehörde die gemeldeten Datennutzungen zwar nicht generell auf ihre Rechtskonformität überprüfen. Im Beschwerdefall bzw im Rahmen von Stichproben sollen Meldungen ans Datenverarbeitungsregister aber geprüft werden.

„Impact Assessments“, also Risikoabschätzungen sollten der Ursprungsabsicht der EU-Kommission zufolge vor dem Beginn der Datenverarbeitung erfolgen und der Öffentlichkeit leicht zugänglich gemacht werden. Davon ist im aktuell leider schon nicht mehr die Rede. Außerdem gehen die Regeln über gut gewählte Überschriften leider kaum hinaus. Sie sind unpräzise und zu unausgereift um Rechtssicherheit zu bieten, wann, in welchem Umfang was zu prüfen ist. Auch die Rolle der Datenschutzbehörde ist unklar. Es ist Vorsorge zu treffen, dass der Datenschutzbehörde Verarbeitungen (die über reine Standardverarbeitungen hinausgehen) auch weiterhin angezeigt werden müssen. Nur so ist gewährleistet, dass sie Datenverantwortliche zu Datenschutz-Folgenabschätzungen auch anhalten kann.

Die Ergebnisse einer Risikoabschätzung müssen ihr auch verpflichtend vorgelegt werden, damit die Behörde bei Bedarf Konsequenzen (in Form von Auflagen oder Empfehlungen) ziehen kann.

19. **Privacy by Design:** Die Anforderungen an den Datenschutz sind schon zum frühestmöglichen Zeitpunkt bei der Entwicklung neuer Technologien zu berücksichtigen. Denn neue Systeme bergen oft Datenschutzrisiken, die sich nur mehr schwer beseitigen lassen, wenn das Grundkonzept erst einmal feststeht. Der Ansatz, Datenschutz ins Gesamtdesign miteinzubeziehen (anstatt Datenschutzprobleme erst später mühsam zu beheben) wird als Privacy by Design bezeichnet. Die Kommissionsvorschläge belieben allerdings zu vage und unverbindlich, um in der Praxis Nutzen zu stiften. Datennutzer sollten konkrete rechtliche Vorgaben beachten müssen, wie bspw.:

- Datenvermeidung: Datenverarbeitung ist so zu dimensionieren, dass keine bzw. nur für den beabsichtigten Zweck unbedingt nötige personenbezogene Daten verwendet werden.
- Kontrolle: IT-Systeme sollten den Betroffenen ermöglichen, ihre Daten aus eigenem zu kontrollieren. Zustimmung bzw. Widersprüche zur Datennutzung sollten technisch vereinfacht werden.
- Transparenz: Entwickler und Betreiber von datenschutzsensiblen Systemen müssen die Betroffenen detailliert über die Funktionsweise der Systeme informieren.
- Vertraulichkeit: nur autorisierte Personen dürfen einen Datenzugriff erhalten.·
- Datenqualität: auch die Datenqualität kann durch technische Mittel unterstützt werden (Prüfung zulässiger Datenquellen und Datenempfänger, Aktualisierungen, Löschroutinen uvm)
- Trennung: werden Systeme für mehrere Zwecke oder von verschiedenen Datennutzern verwendet (z. B. data warehouses, cloud computing) muss gewährleistet, dass diese Datenbestände technisch getrennt aufbewahrt werden.

20. **Privacy by Default:** „Privacy by Default" ist ein Entwicklungskonzept für Software, dass die Sammlung, Offenlegung oder Weitergabe von persönlichen Daten ohne ausdrückliche Zustimmung des Betroffenen verhindern soll. Auch hier bleiben die Vorschläge zu unverbindlich, um wirklich dem Schutz von Internetnutzern zu dienen. Plattformbetreiber müssen zB möglichst konkret verpflichtet werden, die Standardeinstellungen eines Profils in sozialen Netzwerken datenschutzfreundlich zu gestalten. Denn viele Dienstnutzer setzen sich nicht mit komplizierten Privatsphäre-Konzepten, die sie selbst (de-) aktivieren können, auseinander. Die Diensteanbieter profitieren wiederum von Voreinstellungen, mit denen sie die größtmögliche Veröffentlichung bzw. Weitergabe von Daten verwirklichen.

Die Grundeinstellungen für die Privatsphäre eines Dienstes müssen also standardmäßig so restriktiv sein, dass Datenzugriffe minimiert werden.

21. **Pflicht zur Meldung schwerwiegender Datenpannen:** Diese Meldepflicht sollte selbstverständlich sein, um der Datenschutzbehörde die rasche Einleitung eines amtswegigen Prüfverfahrens zu ermöglichen und Betroffene solcherart (aber auch durch eine individuelle Verständigung) vor weitergehenden Schäden zu bewahren und die Durchsetzung allfälliger Ansprüche zu erleichtern. Für die vom Rat geforderten Ausnahmen von der Pflicht zur Meldung schwerwiegender Datenpannen gibt es keine sachliche Rechtfertigung. Ausnahmen wie, „der Auftraggeber hat ohnedies technische Schutzmaßnahmen ergriffen“, ist entgegenzuhalten, dass sie sich aber offenbar als wirkungslos erwiesen haben. Auch wenn der Auftraggeber Maßnahmen ergriffen hat, die sicherstellen, dass „die Betroffenen nicht länger ernsthaft durch die Datenschutzverletzung berührt sind“ haben die Betroffenen ein Infobedürfnis in Bezug auf die zurückliegende Verletzung der Geheimhaltung ihrer Daten. Und selbst wenn die Meldung „wichtigen öffentlichen Interessen widerspricht“, sollte Transparenz gegenüber den Geschädigten vorgehen.

22. **Wirksame Rechtsdurchsetzung:** Für eine wirksame Rechtsdurchsetzung braucht es eine Kombination aus mehreren Mechanismen: Transparenz durch ein vereinfacht zu führendes Datenverarbeitungsregister, eine Risikominimierung heikler Datennutzungen durch behördliche Vorabkontrolle und parallel dazu eine stärkere Verlagerung des (Kosten-) Aufwands auf die Datenverarbeiter selbst (die Datenschutzbehörden sollen die Vorlage von Zertifizierungen, Risikoanalysen uä verlangen können). Neben dem Vertretungsrecht in datenschutzrechtlichen Verfahren sollte Einrichtungen, die die Interessen von ArbeitnehmerInnen und VerbraucherInnen wahrnehmen, eine Verbandsklagsbefugnis zukommen.

23. **Ausgereifte Datenschutz-Folgenabschätzung:** Problematisch an der von der EU-Kommission angestrebten Datenschutz-Folgenabschätzung bleibt, dass diese durch die Datennutzer selbst vorgenommen würde. Diese hätten es sonst - ohne externe Kontrolle - in der Hand, die Gefährdung und Eingriffsintensität der von ihnen betriebenen Anwendungen selbst zu beurteilen und dementsprechend Maßnahmen (wie etwa die Heranziehung der Datenschutzbehörde) zu ergreifen – oder auch nicht. Publizität und Kontrolle wären damit weitgehend ausgeschaltet. Es verbliebe nur die allgemeine Überwachungsbefugnis der Datenschutzbehörden. Aufgrund chronischer finanzieller und personeller Ausstattungsmängel sichert dieses Konzept aber bestenfalls punktuelle Kontrolle. Auch bei einer betriebsinternen Folgenabschätzung ist daher die Datenschutzbehörde formell einzubinden und mit Kontroll- und Gestaltungsrechten auszustatten.

24. **Behördenzuständigkeit ohne One-Stop-Shop**: Das Konzept der ausschließlichen Zuständigkeit der Datenschutzbehörde am Ort der Hauptniederlassung würde den Betroffenen den Zugang zum Recht massiv erschweren. Mit der freien Wahl der „Hauptniederlassung" bleiben Datenschutzbehörden weiterhin Spielball von Konzernen. Nicht nur die zentrale Verwaltung innerhalb der EU, sondern auch der Ort, an dem Entscheidungen über „die Zwecke und Maßnahmen der Datenspeicherung" getroffen werden, wären für die örtliche Zuständigkeit maßgeblich. Das Vorhaben hätte zur Folge, dass zuständige Behörde für ein beispielsweise in Österreich angesiedeltes Tochterunternehmen eines europaweit agierenden Konzerns nicht mehr die österreichische Datenschutzbehörde wäre, sondern die Datenschutzbehörde am Ort der ausländischen Hauptniederlassung des Konzerns. Damit kann ein in mehreren Mitgliedstaaten niedergelassenes Unternehmen leicht Forumshopping zugunsten des Landes mit dem schwächsten Vollzug betreiben.

    Zwar können sich Betroffene weiterhin an ihre nationale Datenschutzbehörde als Anlaufstelle wenden, dieser käme aber keine Entscheidungsbefugnis im Falle von konzernweiten Datenverwendungen zu. An die Entscheidung der „leading"- Datenschutzbehörde wäre auch das nationale Gericht gebunden. Das Modell ist allgemein, vor allem aber im Zusammenhang mit dem Beschäftigtendatenschutz abzulehnen. In die EU-Datenschutz-Grundverordnung sollte deshalb zumindest im Zusammenhang mit dem Beschäftigtendatenschutz deshalb explizit eine Regelung aufgenommen werden, wonach die Zuständigkeit jener Datenschutzbehörde erhalten bleibt, in deren Mitgliedstaat das jeweilige Tochter-Unternehmen als Arbeitgeber der Beschäftigten fungiert. Klarzustellen ist, dass auch den betrieblichen ArbeitnehmerInnen-Interessenvertretungen die Befugnis zukommt, sich zur Wahrnehmung und Durchsetzung datenschutzrelevanter ArbeitnehmerInneninteressen an die Datenschutzbehörde des Niederlassungsortes des jeweiligen Arbeitgebers wenden zu können und antragsberechtigt zu sein.

25. **Behördliche Vorabgenehmigungen:** BürgerInnen wünschen sich einen bestmöglichen vorsorglichen Schutz ihrer Daten. Die nachträgliche Feststellung von Verstößen und allfällige Ersatzleistungen können wirksame Präventivmaßnahmen nicht ersetzen. Dem Kommissionsentwurf zufolge hat der „Verantwortliche vor der Verarbeitung…eine Genehmigung der Aufsichtsbehörde einzuholen, um sicherzustellen, dass die geplante Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt, und insbesondere die Risken (bei Drittlandsübermittlungen) zu mindern….". Vom Rat geplante Streichungen ist eine Absage zu erteilen. Eine Vorabgenehmigung bei besonders sensiblen Datenanwendungen ist dringend notwendig, da eine bloße ex-post Aufsicht das bisherige Datenschutzniveau noch weiter senken würde.

26. **Datenschutzbehörde als „Consultant“:** Absolut zu unterstützen ist der Ansatz von EU-Kommission und EU-Parlament, dass ratsuchende Datenverarbeiter die Datenschutzbehörde auch (gegen Kostenersatz) konsultieren können. Abseits förmlicher und auf dem Rechtsweg bekämpfbarer Behördenentscheidungen muss die Möglichkeit eines institutionalisierten Dialogs zwischen den Datenverarbeitern und ihrer Aufsichtsbehörde bestehen. Die Einholung von Expertise ist in einer von kleinen Unternehmen geprägten Wirtschaftslandschaft enorm wichtig, sollen viele Vorschriften nicht auch aus Überforderung unbeachtet bleiben.

    Vom Rat werden jedoch verbindliche Konsultationen abgelehnt. Die Aufsichtsbehörde sollte nämlich eine Liste an Verarbeitungen erstellen, die Gegenstand der vorherigen Zurateziehung sind und hätte diese zu veröffentlichen gehabt. Eine Pflicht zur Vorabberatung ist unbedingt erforderlich, um den bisherigen enormen Vollzugsdefiziten wirksam zu begegnen.

27. **Verpflichtende betriebliche Datenschutzbeauftragte:** Die verpflichtende Einführung eines betrieblichen Datenschutzbeauftragten in der Privatwirtschaft sollte ein Kernstück jeder ernstzunehmenden Datenschutzreform sein. Der weitgehend freie Datenfluss innerhalb der europäischen Wirtschaft legt eine einheitliche EU-Regelung nahe. Das Abgehen von einer verpflichtenden EU-weiten Einführung hin zu einer bloßen Option für den nationalen Gesetzgeber würde bedeuten, dass die Vereinheitlichung des Datenschutzrechtes in einem überaus zentralen Punkt gescheitert ist. Damit würde die Frage einhergehen, ob der Verordnungscharakter des Rechtsaktes gerechtfertigt ist und nicht einer (Mindestharmonisierungs-) Richtlinie der Vorzug zu geben ist. Vorschläge, ihn nur in Unternehmen mit mehr als 250 MitarbeiterInnen vorzusehen (EU-Kommission) oder ab 5000 von der Datennutzung Betroffenen (EU-Parlament), gehen am Schutzbedürfnis des Einzelnen vorbei. Für die Bedürfnisse von ArbeitnehmerInnen aber auch KonsumentInnen ist eine obligatorische Einsetzung eines Datenschutzbeaufragten in möglichst vielen Unternehmen (bspw. mit mehr als 20 MitarbeiterInnen) weiterhin der beste Garant für die Sicherstellung eines Datenschutzes auf hohem Niveau. Soweit eine EU-weite Einigung völlig außer Reichweite liegt, muss wenigstens eine Melderegisterpflicht bestehen. Eine „weder-noch-Variante“ würde den Wirtschaftsinteressen maximal entgegenkommen ohne aber ein Gleichgewicht mit den legitimen Datenschutzinteressen der Betroffenen herzustellen.

28. **Verpflichtende Datenschutz-TÜVs:** Die softe Förderung von Datenschutzzertifizierungen greift zu kurz. In Bezug auf datenschutzsensible Datenanwendungen muss die Zertifizierung verpflichtender Standard sein. Ohne diesen Schritt wird die Verordnung der Maxime, die Datenschutzregeln fit für das 21. Jahrhundert zu machen, nicht gerecht. „Datenschutz-TÜVs" gelten schon lange als pragmatische Lösung für die ungeheuer großen Vollzugsdefizite im Datenschutzbereich. Datenverarbeiter sollen demnach sensible Vorhaben auf eigene Kosten durch unabhängige Begutachtungsstellen prüfen lassen. Damit kann Datenschutzkonformität im Großen und Ganzen gewährleistet werden (ob ein Vorhaben als datenschutzrechtlich „heikel" einzustufen ist, sollten die Datenschutzbehörden entscheiden). Die Datenschutzbehörden können nicht Millionen registrierter Datenanwendungen gleichzeitig im Auge behalten und sind derzeit auf Beschwerden angewiesen. Viele Verarbeitungen finden aber ohne Wissen der KonsumentInnen „hinter den Kulissen" statt, weshalb nicht allein auf das Einlangen von Anzeigen gesetzt werden kann.

29. **Datenübermittlungen außerhalb der EU:** Im Lichte der zahllosen Datenschutzverletzungen, die die USA - inzwischen hinreichend belegt - systematisch begehen, kann das bisherige System, das auf Gleichwertigkeitsentscheidungen, Standardvertragsklauseln und „Binding Corporate Rules" aufbaut, deren Einhaltung aber niemals geprüft wird, keinesfalls weitergeführt werden. Vor dem Hintergrund des in der Praxis als relativ wertlos geltenden „Safe Harbour-Abkommens" mit der USA führt letztlich kein Weg daran vorbei, Datentransfers in bestimmte Länder, die über kein gleichwertiges Datenschutzniveau verfügen, zu beschränken.

30. **Abschreckende Verwaltungsstrafen**: Nach den ersten Kommissionsplänen sollten die Datenschutzbehörden drakonische Strafen verhängen können: abgestuft bei leichten schuldhaften Verstößen zwischen 100 und 300.000 Euro sowie bei schweren schuldhaften Verstößen zwischen 100.000 Euro und 1.000.000 Euro oder bis zu 5 Prozent des Jahresumsatzes eines Unternehmens (etwa bei rechtswidrigen Datennutzungen, unwirksamen Zustimmungserklärungen). Im offiziellen Entwurf wurde das Vorhaben abgeschwächt: bei erstmaligen „unabsichtlichen" Verstößen eines Unternehmens mit bis zu 250 Beschäftigten soll der Datennutzer nur verwarnt werden. Abschreckende Strafen sind so gut, wie sie vollzogen werden. Wird die Strafgewalt bspw. wegen der Unterfinanzierung der Behörden kaum angewendet, so bleibt die Wirkung einer – wenn auch hohen – Strafdrohung in der Praxis gering.

31. **Behördenkooperation:** Die Kooperationsregeln im Falle von Beschwerden an eine Datenschutzbehörde, die mehrere Mitgliedstaaten berühren, sind derart komplex geraten, dass mit einer Sachverhaltsklärung und Entscheidung innerhalb angemessener Frist kaum zu rechnen ist.

Außerdem ist fraglich, wie sämtliche Äußerungsrechte und Einwandmöglichkeiten für alle beteiligten Behörden und einen europäischen Datenschutzausschuss verfahrensrechtlich zu qualifizieren sind. Die nationalen Datenschutzbehörden werden dadurch auch von nationalen Strukturen und demokratischer Legitimation schrittweise entkoppelt. Die Rechtsschutzmöglichkeiten für die Betroffenen müssen jedenfalls an ihrem Wohnsitzort in jeder Hinsicht gewahrt bleiben.

32. **Detailregeln für spezifische Datennutzungen:** Die Anforderungen in Bezug auf die Nutzung von Gesundheitsdaten, ArbeitnehmerInnendaten, soziale Sicherheit usw. sind zum Teil so spezifisch, dass rudimentäre Regeln in einer EU-Verordnung nicht ausreichen. In all diesen Fällen bedarf es der Klarstellung, dass der nationale Gesetzgeber – abgehend vom Vollharmonisierungscharakter der Verordnung in diesen Bereichen - nicht daran gehindert ist, in diesen Regelungsbereichen abweichende vor allem datenschutzrechtlich strengere Normen zu erlassen.

33. **Verbesserung des Datenschutzes für ArbeitnehmerInnen in Europa:**

In Österreich aber auch auf EU-Ebene gibt es kaum spezifische Vorschriften, die auf das besondere Schutzbedürfnis der Beschäftigten im Arbeitsverhältnis Bedacht nehmen. Auch der EU-Entwurf zu einer Datenschutzverordnung geht kaum auf die Besonderheiten von Arbeitsverhältnissen ein. Zum Teil sind sogar Verschlechterungen für die Rechtsdurchsetzung von Betriebsräten und Beschäftigten zu befürchten. Adäquate Datenschutzbestimmungen für ArbeitnehmerInnen und eine effiziente Rechtsdurchsetzung zum Schutz von Beschäftigtendaten im betrieblichen Kontext sollten in Angriff genommen werden. Dazu zählt:

- Die Anforderungen in Bezug auf die Nutzung von ArbeitnehmerInnendaten sind zum Teil sehr spezifisch. Es muss daher im geplanten Art 82 der Datenschutz-Grundverordnung klargestellt werden, dass der nationale Gesetzgeber nicht daran gehindert ist, in diesem Regelungsbereich abweichende vor allem datenschutzrechtlich strengere Normen zu erlassen.

- Insbesondere dürfen die Europäischen Datenschutzregelungen die nationalen Arbeitsverfassungen (d.h. die Rechte der betrieblichen und überbetrieblichen Interessenvertretungen) nicht berühren. Sie dürfen diese folglich auch nicht in ihrer Gültigkeit beschränken und bestehende Betriebsratsrechte beschneiden.

- In einem europäischen Regelwerk sollen auch Arbeitnehmervertretungen (zB Konzernbetriebsrat, europäischer Betriebsrat) berücksichtigt werden, indem etwa bei der Zulässigkeit von Datenübermittlungen auf den Abschluss von Betriebsvereinbarungen abgestellt wird statt auf das Vorhandensein einseitig erlassener Arbeitgeberrichtlinien.

- Arbeiterkammern und Gewerkschaften sollen zu den in Datenschutzangelegenheiten (verbands-)-klagsberechtigten Einrichtungen gehören.

- Statt dem One-Stop-Shop - Prinzip muss die Zuständigkeit der nationalen Datenschutzbehörde gewährleistet sein. Denn das im Entwurf zur Datenschutzverordnung vorgesehene One-Stop-Shop – Verfahren hätte zur Folge, dass zuständige Behörde für ein beispielsweise in Österreich angesiedeltes Tochterunternehmen eines europaweit agierenden Konzerns nicht mehr die österreichische Datenschutzbehörde wäre, sondern dass die Datenschutzbehörde am Ort der ausländischen Hauptniederlassung des Konzerns die Entscheidung über die Zulässigkeit einer Datenanwendung trifft. Damit würde Arbeitnehmern des österreichischen Tochterunternehmens zum einen der Zugang zum Recht massiv erschwert. Zum anderen werden Konzerne wohl die Tendenz haben, ihre Hauptniederlassung in dem Mitgliedstaat einzurichten, in dem faktisch das schwächste Rechtschutzniveau (inkl. des Datenschutzrechts) herrscht.

  Sind ArbeitnehmerInnen, betriebliche Interessenvertretungen und Datenschutzbeauftragte in (Tochter-)Unternehmen von mutmaßlichen Verstößen eines (Konzern-)Unternehmens in einem anderen Mitgliedstaat betroffen, sollten sie sich mit Beschwerden (auch) an die Datenschutzbehörde desjenigen Mitgliedstaates wenden können, in dem das jeweilige (Tochter-) Unternehmen als Arbeitgeber der Beschäftigten fungiert. Nach Wahl des Arbeitnehmers/der Arbeitnehmerin sollte (auch) die Datenschutzbehörde des Mitgliedstaates des Ortes seiner/ihrer gewöhnlichen Beschäftigung angerufen werden können. Die federführende Datenschutzbehörde im Mitgliedstaat der Hauptniederlassung des Datenverwenders soll sich mit den Datenschutzbehörden in anderen Mitgliedstaaten, in denen Betroffene beschäftigt werden, koordinieren müssen. Sind Rechtsfragen zwischen den beteiligten Datenschutzbehörden strittig, soll der EUGH anzurufen sein.

  Klarzustellen ist, dass auch den betrieblichen ArbeitnehmerInnen-Interessenvertretungen die Befugnis zukommt, sich zur Wahrnehmung und Durchsetzung datenschutzrelevanter ArbeitnehmerInneninteressen an die Datenschutzbehörde des Niederlassungsortes des jeweiligen Arbeitgebers wenden zu können und antragsberechtigt zu sein.

- Es muss außerdem ein betrieblicher Datenschutzbeauftragter vor Ort vorhanden sein. Ein Konzerndatenschutzbeauftragter nur am Ort der Hauptniederlassung des Konzerns kann allein den Betriebsräten in diversen Tochterunternehmen nicht als Ansprechpartner dienen. Wichtig wäre daher die verpflichtende Bestellung eines betrieblichen Datenschutzbeauftragten ab einer möglichst niedrigen Beschäftigtenanzahl. Generell sind Ausnahmen für kleine und mittlere Unternehmen in Bezug auf den Grundrechtsschutz kritisch zu hinterfragen. Der Schutz der persönlichen Daten der Beschäftigten muss auch in kleinen Betrieben ohne Abstriche gewahrt bleiben. Wie oben angeführt ist zudem eine Vertretungsbefugnis des Betriebsrats als betriebliche Interessenvertretung seiner ArbeitnehmerInnen in datenschutzrechtlichen Angelegenheiten nötig.

- Erforderlich ist auch ein Beweisverwertungsverbot für unrechtmäßig erlangte Personaldaten, um dem Trend, sich ohne nennenswerte praktische Konsequenzen unfaire Vorteile durch Datenschutzverstöße verschaffen zu können, wirksam zu begegnen.

- Die Wirksamkeit von datenschutzrechtlichen Einwilligungserklärungen (von Arbeitnehmern) im Arbeitsverhältnis ist zu beschränken. Auf Grund des typischen Verhandlungsungleichgewichts im Arbeitsverhältnis erklären sich ArbeitnehmerInnen oft notgedrungen zur Einwilligung bereit und trauen sich aus Angst um ihren Arbeitsplatz in der Folge nicht, diese zu widerrufen.

- Im Falle schwerwiegender Datenschutzverletzungen (wie etwa Datenmissbrauch oder –verlust) kann durch eine uneingeschränkte Infopflicht des Auftraggebers die Transparenz (unabhängig von einem - schwer abschätzbaren - drohenden Schadenseintritt bei den Betroffenen) gegenüber Betroffenen und der Datenschutzbehörde verbessert werden.

- Nötig sind Regeln zum externen Whistleblowing. Wenn gewünscht wird, dass Missstände im Betrieb von Beschäftigten der zuständigen Behörde gemeldet werden, so müssen diese vor arbeitsrechtlichen Nachteilen – Kündigungsverbot, Benachteiligungsverbot - geschützt werden.

- Benötigt werden auch internationale Regeln, die sicherstellen, dass Personaldaten in einem rechtlich gesicherten Rahmen grenzüberschreitend transferiert werden und Ansprüche auch im Ausland durchsetzbar sind.