# Grundzüge des Schutzes der personenbezogenen Daten in der geltenden Gesetzgebung Italiens

*Barbara Pusateri*



## I. Prämissen

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht im Rahmen der Rechtsordnung der Europäischen Union. Das besagt nicht nur **Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union, der so genannten Charta von Nizza,** sondern auch **Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)**, in denen das Recht jeder Person auf den Schutz personenbezogener Daten verankert ist.

Die Entwicklung neuer Technologien im Zusammenhang mit der inzwischen anerkannten Globalisierung von Diensten und Informationen erfordert einen wirksameren Schutz personenbezogener Daten bei deren Verarbeitung, der sich von den bisher angewandten Schutzmaßnahmen deutlich abhebt.

Bereits die Richtlinie 95/46/EG[1] hatte zum Ziel, den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung zu harmonisieren und den freien Verkehr personenbezogener Daten zwischen den Mitgliedstaaten zu gewährleisten. Diese Richtlinie stellte somit lange Zeit das wichtigste Rechtsinstrument der Europäischen Union im Bereich des Datenschutzes dar.

Trotz dieses ehrgeizigen Zieles wies die Richtlinie 95/46/EG bei ihrer Anwendung einige Mängel auf. Der Hauptgrund dafür lag darin, dass es sich bei der Richtlinie um einen Rechtsakt handelte, der nicht in seiner Gesamtheit verbindlich war, da er nur verbindliche Zielvorgaben für die Mitgliedsstaaten enthielt. Es war anschließend die Aufgabe eines jeden Mitgliedstaates, durch nationale Bestimmungen festzulegen, wie diese Ziele erreicht werden sollen.

[1] Veröffentlicht im Amtsblatt Nr. L 281 vom 23/11/1995 S 0031 - 0050.

Der weite Spielraum, welcher der Gesetzesinitiative überlassen wurde, führte zu Unterschieden zwischen den Mitgliedstaaten bei der Umsetzung und Anwendung der Richtlinie 95/46/EG, was wiederum zu Unsicherheiten hinsichlich der angewandten Schutzstandards führte.

Die kritischen Punkte im Hinblick auf die Wirksamkeit des durch die oben genannte Richtlinie gebotenen Rechtsschutzes haben den europäischen Gesetzgeber dazu veranlasst, zur Regelung eines derart heiklen und vielschichtigen Sachbereiches, wie jenen des Datenschutzes, ein anderes, die Rechtsordnung der EU prägendes Rechtsinstrument anzuwenden, nämlich die Verordnung. Die Verordnung hat eine größere Wirkung als die Richtlinie, zumal alle Elemente derselben verbindlich und ihre Bestimmungen auf alle Mitgliedstaaten direkt anwendbar sind.

Demnach ermöglicht die Anwendung der Verordnung in diesem Sachbereich, einen einheitlichen Schutzstandard für personenbezogene Daten in der gesamten Europäischen Union zu gewährleisten und somit wesentliche Unterschiede zu vermeiden, die den freien Verkehr dieser Daten im Binnenmarkt behindern könnten.

## II. Die Datenschutz-Grundverordnung EU-Verordnung Nr. 2016/679 und das gesetzesvertretende Dekret Nr. 101/2018

Auf der Grundlage dieser Überlegungen verabschiedeten das Europäische Parlament und der Europäische Rat am 26. April 2016 die Verordnung 679/2016[2] zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG. Diese Verordnung, kurz als **Datenschutz-Grundverordnung (DSGVO)** bezeichnet, trat am 24. Mai 2016, zwanzig Tage nach deren Veröffentlichung im Amtsblatt der Europäischen Union, in Kraft und ist seit 25. Mai 2018 verbindlich anzuwenden.

Die EU-Verordnung Nr. 2016/679 hat einen solideren und konsequenteren Rechtsrahmen für den Datenschutz geschaffen.

In Umsetzung der in Art. 13 des Gesetzes Nr. 163 vom 25. Oktober 2017 enthaltenen Ermächtigung der Regierung zur Anwendung der EU-Richtlinien 2016 - 2017 hat der italienische Staat ein gesetzesvertretendes Dekret zur Anpassung der nationalen Gesetzgebung zum Schutz personenbezogener Daten erlassen. Es handelt sich dabei um das gesetzesvertretende Dekret Nr. 101 vom 10. August 2018 „Bestimmungen zur Anpassung der nationalen Gesetzgebung

[2] Veröffentlicht im Amtsblatt Nr. L 119 vom 4/5/2016 S 1-88.

an die Bestimmungen der EU-Verordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie Nr. 95/46/EG", veröffentlicht am 4. September 2018 im Gesetzesanzeiger der Republik Italien Nr. 205/2018. Damit wurden die Bestimmungen des gesetzesvertretenden Dekrets Nr. 196 „Kodex zum Schutz personenbezogener Daten" vom 30. Juni 2003 aufgehoben, da sie mit der Datenschutz-Grundverordnung unvereinbar waren. Es sind nicht nur neue Bestimmungen eingeführt, sondern auch die weiterhin geltenden Bestimmungen ergänzt und überarbeitet worden.

Hauptzweck des vormals geltenden Datenschutzkodex war es, die Verarbeitung von Daten ohne Zustimmung des Rechtsinhabers oder in einer Weise, die ihn schädigt, zu verhindern. Darüber hinaus war darin auch die Ergreifung technischer und organisatorischer Vorkehrungen vorgesehen, die alle befolgen mussten, um die Daten Dritter ordnungsgemäß zu verarbeiten. Auch sollte das Risiko des Verlusts und der Zerstörung von Daten dadurch minimiert werden, dass „Mindestsicherheitsmaßnahmen" vorgeschrieben wurden, die von jedem, der personenbezogene Daten Dritter verarbeitete, getroffen werden mussten (Mindestmaßnahmen wie zB die Verwendung von Authentifizierungscodes für den Zugang zu den Daten oder die Einrichtung und Verwaltung von Datensicherungen).

Im Falle einer Verletzung der Rechte an den eigenen Daten (zB Erhebung von Daten ohne Einwilligung, Einholung einer Einwilligung ohne vorherige rechtliche Aufklärung, Verarbeitung der Daten über die Grenzen der Einwilligung hinaus, Verweigerung oder Einschränkung des Zugangs zu den Daten) sah der Datenschutzkodex die Möglichkeit vor, sich an die Datenschutzbehörde oder alternativ an das Gericht zu wenden.

Mit dem gesetzesvertretenden Dekret zur Anpassung der staatlichen Rechtsvorschriften an die Bestimmungen der EU-Verordnung Nr. 679/2016 wurde der alte Datenschutzkodex nicht nur in seinen Bestimmungen grundlegend novelliert, sondern auch in seiner Grundausrichtung und seinen Zielsetzungen wesentlich überarbeitet. Der Datenschutzkodex und die EU-Verordnung stützen sich auf zwei unterschiedliche Denkschulen. Wie bekannt, fußt die EU-Verordnung auf dem Grundsatz der Rechenschaftspflicht. Nach diesem Grundsatz ist es die Aufgabe der Verantwortlichen für die Datenverarbeitung, die Einhaltung der für die Verarbeitung personenbezogener Daten geltenden Grundsätze sicherzustellen und nachzuweisen. Das bedeutet, dass die Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer nachvollziehbaren Weise verarbeitet werden müssen. Außerdem dürfen die Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und

müssen auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt und sachlich richtig sein. Die Daten dürfen nur zeitlich begrenzt gespeichert werden. Bei der Verarbeitung der Daten sind deren Sicherheit und Unversehrtheit zu gewährleisten. Die EU-Verordnung überlässt dem Verantwortlichen die Wahl: Er ist dazu aufgerufen, eine Bewertung durchzuführen, eine Entscheidung zu treffen und nachzuweisen, dass er angemessene und wirksame Maßnahmen getroffen hat. Es ist daher die Pflicht des Verantwortlichen für die Datenverarbeitung nachzuweisen, dass er ein angemessenes „Organisationsmodell für den Datenschutz" eingerichtet hat.

In der EU-Verordnung wird also eine Ex-Ante-Herangehensweise „durch Technikgestaltung" (sog. „by design") verlangt, dh. die Datenverarbeitung soll von Vornherein gesetzeskonform erfolgen. Der ehemalige Datenschutzkodex ging hingegen von einem Ex-Post-Ansatz aus, dh. mit der Datenverarbeitung befasste man sich erst im Nachhinein, beim Auftreten eines Problems. Man kann also behaupten, dass der oben genannte Datenschutzkodex spezifischere Regeln enthielt, während die EU-Verordnung auf allgemeinen Regeln fußt, die vom einzelnen Verantwortlichen anhand der jeweiligen Umstände zu bewerten sind.

Der Sinn und Zweck des gesetzesvertretenden Dekrets Nr. 101/2018 besteht im Wesentlichen darin, die vom italienischen Gesetzgeber im Datenschutzkodex (des gesetzesvertretenden Dekrets Nr. 196/2003) festgelegten Regeln mit denen der EU-Verordnung in Einklang zu bringen.

Das gesetzesvertretende Dekret Nr. 101/2018 ist in sechs Abschnitte gegliedert und umfasst 27 Artikel, die verschiedene Aspekte des Datenschutzes betreffen.

## III. Wesentliche Bestimmungen des gesetzesvertretenden Dekretes Nr. 101/2018

Es folgt eine Erläuterung der wesentlichen Bestimmungen des gesetzesvertretenden Dekrets Nr. 101/2018:

- **Rechtsgrundlage für die Wahrnehmung von Aufgaben im öffentlichen Interesse oder in der Ausübung öffentlicher Gewalt:** Bei Datenverarbeitungen, die „im Rahmen der Wahrnehmung von Aufgaben im öffentlichen Interesse oder in der Ausübung öffentlicher Gewalt" erfolgen, liegt die Rechtsgrundlage für die Verarbeitung „allgemeiner" personenbezogener Daten laut Art. 2-ter der Novelle zum Datenschutzkodex ausschließlich in einer Gesetzes- oder Verordnungsbestimmung. Demnach kann die Verarbeitung gerichtlicher Daten im öffentlichen Bereich, zB im Rahmen der Durchführung von Auftragsvergaben, nur bei Vorliegen einer

geeigneten Rechtsgrundlage (zB Vergabekodex und entsprechender Rechtsvorschriften der Autonomen Provinz Bozen-Südtirol) erfolgen.

- **Deontologische Vorschriften:** Der staatliche Gesetzgeber hat die Verhaltenskodexe (nun in „deontologische Vorschriften" umbenannt) beibehalten. Diese müssen überarbeitet, an die EU-Verordnung angepasst und zu einem späteren Zeitpunkt von der Datenschutzbehörde genehmigt werden. Es ist daher Aufgabe der Datenschutzbehörde, die Einführung deontologischer Vorschriften für die Verarbeitung personenbezogener Daten in bestimmten Bereichen (Arbeit, Journalismus, Statistik und wissenschaftlicher Forschung) unter Miteinbeziehung der Interessengruppen und nach Durchführung einer öffentlichen Befragung zu fördern.
- **Zustimmung des Minderjährigen:** Gemäß Art. 2-quinquies der Novelle zum Datenschutzkodex kann ein Minderjähriger ab 14 Jahren in Anwendung des dritten Satzes von Art. 8 Abs. 1 der Datenschutz-Grundverordnung der Verarbeitung seiner personenbezogenen Daten im Zusammenhang mit der direkten Erbringung von Dienstleistungen der Informationsgesellschaft zustimmen (die EU-Verordnung sieht hingegen eine Altersgrenze von 16 Jahren vor). Für Minderjährige unter dieser Altersgrenze müssen die Eltern oder die Sorgeberechtigten ihre Zustimmung erteilen. Laut Art. 2-quinquies Abs. 2 ist der Verantwortliche dazu verpflichtet, die Informationen und Mitteilungen über das an Minderjährige gerichtete Dienstleistungsangebot der Informationsgesellschaft in „*besonders klarer und einfacher Sprache, prägnant und ausführlich, leicht verständlich und für den Minderjährigen nachvollziehbar*" zu verfassen. Dadurch soll gewährleistet werden, dass der Minderjährige seine Zustimmung bewusst erteilt.
- **Verarbeitung besonderer Kategorien von personenbezogenen Daten aus Gründen des öffentlichen Interesses:** Besondere Kategorien von personenbezogenen Daten (in Italien auch als „sensible Daten" bekannt) dürfen ausschließlich bei Vorliegen bestimmter Voraussetzungen verarbeitet werden, etwa bei Vorliegen eines öffentlichen Interesses oder bei Ausübung öffentlicher Gewalt (zB Erhebung des Gesundheitszustandes im Hinblick auf den Erwerb des Führerscheins).
- **Garantiemaßnahmen für genetische, biometrische und gesundheitliche Daten:** Genetische, biometrische und gesundheitliche Daten, für die in den Gesetzen der einzelnen Mitgliedsstaaten zusätzliche Bedingungen gelten können (Art. 9 Abs. 4 der Datenschutz-Grundverordnung), dürfen im Hinblick auf die Verfahren für den physischen und elektronischen Zugriff zu den Daten durch Befugte unter Einhaltung von Garantiemaßnahmen verwendet werden, die von der

Datenschutzbehörde mit einer mindestens alle zwei Jahre getroffenen Maßnahme angeordnet werden (sensible Daten müssen im Unterschied zu allgemeinen Daten zusätzlichen Sicherheitsmaßnahmen - wie etwa einer Verschlüsselung oder einem Kennwortschutz - unterliegen). Die Datenschutzbehörde hat also die Aufgabe, die Garantiemaßnahmen für die Verarbeitung von genetischen, biometrischen und gesundheitlichen Daten zu erarbeiten. Die Garantiemaßnahmen für genetische Daten und für die Verarbeitung von Gesundheitsdaten zum Zwecke der Prävention, Diagnose und Behandlung werden nach Rücksprache mit dem Gesundheitsministerium beschlossen, das zu diesem Zweck die Stellungnahme des Obersten Gesundheitsrates einholt.

- **Einschränkung der Rechte betroffener Personen:** Die Ausübung der Rechte durch die betroffene Person kann eingeschränkt werden, wenn dadurch ein übergeordnetes Interesse, dh. ein gesetzlich geschütztes Interesse, gefährdet ist (zB Verteidigung von Rechtsansprüchen vor Gericht, Unabhängigkeit der Gerichtsbarkeit, Geldwäschebekämpfung).
- **Verarbeitung der Daten verstorbener Personen:** Es wird der Begriff des Rechts auf Vererbung von Daten im Todesfall eingeführt. Eine neue Vorschrift ermöglicht es jedem, zu verfügen, was mit den eigenen Daten, die in den Informationsdiensten von Unternehmen gespeichert sind, nach dem eigenen Ableben geschehen soll. Mit Bezug auf die Daten von Verstorbenen können die Rechte der betroffenen Person laut Art. 2-terdecies von all denjenigen geltend gemacht werden, die ein persönliches Interesse daran haben oder die zum Schutz der betroffenen Person oder aus schutzwürdigen familiären Gründen handeln. Die Ausübung dieser Rechte ist nicht zulässig, wenn sie gegen das Gesetz verstößt oder wenn die betroffene Person - beschränkt auf die „direkte Erbringung von Diensten der Informationsgesellschaft“ - dies in einer schriftlichen und eindeutigen Erklärung ausdrücklich untersagt hat. Ein Verbot darf sich jedoch nicht nachteilig auf die Ausübung der Eigentumsrechte Dritter, die sich aus dem Tod der betroffenen Person ergeben, oder des Rechtes auf Verteidigung ihrer Interessen vor Gericht auswirken.
- **Vereinfachte Regelung für kleine und mittlere Unternehmen:** Die Datenschutzbehörde ist gemäß den Bestimmungen der Datenschutz-Grundverordnung und des neuen Datenschutzkodexes befugt, Vereinfachungsmechanismen für Kleinst-, Klein- und Mittelunternehmen unter Bezugnahme auf die Pflichten des Verantwortlichen einzuführen (zB sind diese Unternehmen nicht verpflichtet, einen Datenschutzbeauftragten zu haben, und dürfen vereinfachte Verarbeitungsregister führen, in denen nur die Verarbeitung kritischer Daten, falls vorhanden, aufgezeichnet wird).

- **Verarbeitung von Daten in Bezug auf Schülerinnen und Schüler:** Mit Zustimmung der betroffenen Person dürfen Daten über die Ausbildung, die Zwischen- und Endergebnisse und andere personenbezogene Daten von Schülerinnen und Schülern, die nicht in den Art. 9 und 10 der Datenschutz-Grundverordnung aufgeführt sind, mitgeteilt oder verbreitet werden (zB kann sich ein Arbeitgeber bei der Schule erkundigen, mit welcher Note eine Bewerberin oder ein Bewerber um eine freie Stelle die Abschlussprüfung bestanden hat). Ziel ist es, die Berufseingliederung (auch im Ausland), die Ausbildung und die Berufsberatung zu erleichtern.
- **Lebenslauf:** Laut Art. 111-bis des gesetzesvertretenden Dekrets Nr. 101/2018 müssen die Informationen gemäß Art. 13 Datenschutz-Grundverordnung bei der ersten sich bietenden Kontaktaufnahme nach der Zusendung des Lebenslaufs übermittelt werden. Im Rahmen der in Art. 6 Abs. 1 lit. b der Datenschutz-Grundverordnung genannten Zielsetzungen ist die Zustimmung des Bewerbers zur Verarbeitung der im Lebenslauf enthaltenen personenbezogenen Daten nicht erforderlich.
- **Formen des Schutzes durch die Datenschutzbehörde:** In der Datenschutz-Grundverordnung ist der Rechtsbehelf als Mittel zur Durchsetzung des Rechts auf Zugang zu personenbezogenen Daten nicht mehr vorgesehen. Daher wurde mit dem gesetzesvertretenden Dekret Nr. 101/2018 die Beschwerde als alternative Schutzform zum gerichtlichen Rechtsbehelf eingeführt. Gemäß Art. 142 der Novelle zum Datenschutzkodex wird das Verfahren zur Bearbeitung von Beschwerden durch die Datenschutzbehörde mit einer eigenen Verordnung geregelt. Die Bearbeitung wird einige Zeit in Anspruch nehmen. Im Art. 143 Abs. 3 wird nämlich klargestellt, dass die Datenschutzbehörde innerhalb von neun Monaten nach der Einreichung der Beschwerde darüber befinden wird; allerdings ist sie innerhalb von drei Monaten nach demselben Datum verpflichtet, die betroffene Person über den Stand des Verfahrens zu informieren.

Die betroffene Person kann die Beschwerde einreichen, wenn sie der Ansicht ist, dass ihre Rechte im Sinne der Datenschutzvorschriften verletzt wurden. In der Beschwerde sind der Tatbestand und die Umstände, auf denen sie beruht, möglichst ausführlich zu schildern und die mutmaßlichen Verstöße, die erwünschten Maßnahmen sowie die Identifikationsdaten des Verantwortlichen oder des Auftragsverarbeiters - soweit bekannt - anzugeben. Der Beschwerde sind alle für ihre Bearbeitung erforderlichen Unterlagen beizufügen. Die Datenschutzbehörde hat unverzüglich (gleich nach Inkrafttreten der Datenschutz-Grundverordnung) ein Beschwerdeformular erstellt und auf seiner institutionellen Webseite veröffentlicht.

Anders als im bisher geltenden Datenschutzkodex vorgesehen, kann nun jede und jeder eine Meldung an die Datenschutzbehörde richten. Nach deren Prüfung kann diese die in Art. 58 der Datenschutz-Grundverordnung genannten Maßnahmen erlassen. Im gesetzesvertretenden Dekret Nr. 196/2003 war diese Möglichkeit ausschließlich der betroffenen Person vorbehalten.

- **Strafen:** Der italienische Gesetzgeber hat von der gemäß Datenschutz-Grundverordnung allen Mitgliedstaaten eingeräumten Möglichkeit Gebrauch gemacht, strafrechtliche Sanktionen für bestimmte Verstöße gegen die Datenschutzbestimmungen vorzusehen, die über die in dieser Verordnung enthaltenen, ohnehin strengen Verwaltungssanktionen hinausgehen. Strafrechtlich verfolgt werden:
  - die rechtswidrige Verarbeitung personenbezogener Daten;
  - der betrügerische Erwerb personenbezogener Daten, die einer umfangreichen Verarbeitung unterliegen;
  - die rechtswidrige Übermittlung und Verbreitung personenbezogener Daten, die einer umfangreichen Verarbeitung unterliegen;
  - falsche Angaben gegenüber der Datenschutzbehörde;
  - die Nichteinhaltung der Bestimmungen der Datenschutzbehörde;
  - Verstöße gegen Art. 4 Abs. 1 des Arbeitnehmerstatuts (Verletzung der Bestimmungen über Fernkontrollen und Untersuchungen über die Meinungen der Arbeitnehmer).

  Was das Sanktionssystem betrifft, ersetzt das gesetzesvertretende Dekret Nr. 101/2018 nach dem strafrechtlichen Grundsatz des Analogieverbots (*favor rei*) die im vorherigen Datenschutzkodex enthaltenen strafrechtlichen Sanktionen durch die in der Datenschutz-Grundverordnung vorgesehene breite Palette an Verwaltungsstrafen auch im Hinblick auf Verstöße, die vor dem Inkrafttreten des Dekrets begangen wurden, und sofern das Strafverfahren nicht durch ein rechtskräftig gewordenes Urteil oder Dekret entschieden wurde.

  Gemäß Art. 22 Abs. 13 des gesetzesvertretenden Dekrets Nr. 101/2018 gilt ab Inkrafttreten des Dekrets eine achtmonatige Phase der Erstanwendung von Sanktionen. Die achtmonatige Frist ab Inkrafttreten des Dekrets ist nur im Hinblick auf die Kriterien von Belang, welche die Datenschutzbehörde bei der Festlegung von Geldstrafen für Verstöße gegen die im Dekret enthaltenen Bestimmungen berücksichtigen muss, und zwar nur insofern, als diese Geldstrafen mit der Datenschutz-Grundverordnung vereinbar sind. Diese Regelung sorgt dafür, dass die Datenschutzbehörde in den ersten acht

Monaten bei der Verhängung von Sanktionen nachsichtiger vorgehen und mehrere Faktoren berücksichtigen wird.

- **Datenschutzbehörde:** Mit dem gesetzesvertretenden Dekret Nr. 101/2018 werden die Befugnisse und Pflichten der Datenschutzbehörde den neuen Gegebenheiten angepasst. Die Datenschutzbehörde ist eine unabhängige Verwaltungsbehörde, die sich aus dem leitenden Kollegium und dem Büro zusammensetzt. Das Kollegium besteht aus vier Mitgliedern, die vom Parlament im Rahmen eines Auswahlverfahrens ernannt werden.

  In Art. 154 des gesetzesvertretenden Dekrets Nr. 101/2018 wird eine Reihe weiterer Aufgaben aufgelistet, die der Datenschutzbehörde übertragen wurden, darunter

  - die Überprüfung, ob die Verarbeitung auch im Falle ihrer Beendigung und unter Berücksichtigung der Speicherung von Verkehrsdaten in Übereinstimmung mit den geltenden Vorschriften erfolgt,
  - die Behandlung von Beschwerden, die gemäß der Datenschutz-Grundverordnung und den Bestimmungen des Datenschutzkodexes eingereicht wurden,
  - die Ausarbeitung spezifischer Bearbeitungsverfahren mit einer eigenen Verordnung,
  - die Festlegung jährlicher Prioritäten für Fragen im Zusammenhang mit Beschwerden, die im Laufe des Jahres bearbeitet werden können,
  - die Initiative zur Genehmigung von deontologischen Vorschriften.

  Gemäß Art. 154-bis der Novelle zum Datenschutzkodex wird der Datenschutzbehörde zudem eine Reihe zusätzlicher Befugnisse erteilt, darunter die Annahme von Leitlinien für organisatorische und technische Maßnahmen zur Umsetzung der Grundsätze der Datenschutz-Grundverordnung auch für einzelne Sachbereiche und in Anwendung der in Art. 25 der Datenschutz-Grundverordnung festgelegten Grundsätze sowie die Genehmigung von deontologischen Vorschriften. Die Datenschutzbehörde kann außerdem die Vertreter einer anderen unabhängigen nationalen Verwaltungsbehörde zur Teilnahme an ihren Sitzungen einladen. Sie ist befugt, gegen den Verantwortlichen oder den Auftragsverarbeiter rechtliche Schritte einzuleiten, wenn diese gegen die Bestimmungen über den Schutz personenbezogener Daten verstoßen. Die Datenschutzbehörde wird vor Gericht durch die Staatsadvokatur vertreten.

  Das Büro der Datenschutzbehörde wird von einem Generalsekretär geleitet, der aus einer Reihe von Personen mit hoher und nachgewiesener fachlicher Qualifikation in Bezug auf die zu erreichenden Aufgaben und Ziele ernannt wird. Das Büro der Datenschutzbehörde ist in Abteilungen und Dienste

gegliedert, die verschiedene Tätigkeitsbereiche abdecken (zB Gesundheits- und Forschungsabteilung, Abteilung für Meinungsfreiheit und Cyber-Bullying, usw.). Der Stellenplan sieht höchstens 162 Personaleinheiten vor.

## IV. Abschließende Überlegungen

In Italien wurde die Datenschutz-Grundverordnung eher als eine erneute bürokratische Auflage aufgefasst, die bei lückenhafter oder mangelnder Umsetzung auf schwerwiegende Weise sanktioniert wird. In Wirklichkeit kann ein verantwortungsvollerer Ansatz bei der Verarbeitung und dem Schutz der personenbezogenen Daten aber eine Möglichkeit darstellen, um die Transparenz und Korrektheit in diesem Bereich bestmöglich zu garantieren. Es handelt sich hierbei um eine Chance, die Gelegenheit zu nutzen, die einzelnen Abläufe zu erheben. Diese Tätigkeit ist auch für die Durchführung anderer gesetzlichen Obliegenheiten wertvoll, insbesondere im Zusammenhang mit der Erstellung von Organisationsmodellen (zB im Rahmen der Korruptionsvorbeugung).