Impulses for an Effective and Modern Data Protection System

by **Niko Härting,** lecturer at the Freie Universität Berlin, founding partner HÄRTING Rechtsanwälte, Berlin
and
Jochen Schneider, honorary professor at the Ludwig-Maximilians-Universität München, founding Partner SSW Schneider Schiffer Weihermüller, Munich

Abstract: A substantial reform of data protection law is on the agenda of the European Commission as it is widely agreed that data protection law is faced by lots of challenges, due to fundamental technical and social changes or even revolutions. Therefore, the authors have issued draft new provisions on data protection law that would work in both Germany and Europe. The draft is intended to provide a new approach and deal with the consequences of such an approach. This article contains some key theses on the main legislatory changes that appear both necessary and adequate.

Keywords: EU Directive on Data Protection; Private Sphere; Privacy by Design;Principle of Prohibition; Freedom of Communication; Free Flow of Data; Sensitive Data; Transparency; Secrecy of Observation; Consent Liability concept

Recommended citation: Härting/Schneider, Impulse für einen effektiven und modernen "Datenschutz", 3 (2011) JIPITEC 195, para 1.

A. Introduction

1 Since 1973 there has been a data protection law in Sweden.[1] Germany's "Federal Data Protection Act" - BDSG[2] dates from 1977. This was preceded, in as early as 1970, by a data protection law for the German Federal State of Hessen.[3] The demand for protection was due to the menace emanating from "mechanical data processing", the central systems and data files. As a result, "personal data" came to the fore as regulatory subject. By way of an anticipated need for protection of a fundamental right, the individual was to be protected, within an initially narrowly defined scope of application, from a situation in which this menace became reality (principle of imposing a ban with permit reservation).

2 Since 1995, there has been a unified data protection regime at EU level in the form of directive 95/46/EC dated 24 October 1995 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data". Article 8 of the EU Charter of Fundamental Rights affords "the protection of personal data" the same level of protection as the Charter's article 11 affords to freedom of expression and information.

3 In the course of time, the BDSG has been amended several times. The aforementioned directive was supplemented by directive 2006/24/EC dated 15 March 2006 on data retention and before that, on 12 July 2002, by directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector, which has also been amended since then. It is safe to say that there

is a largely integrated data protection system within the EU on the abstract level. In concrete terms, however, there are substantial differences which are due to the somewhat divergent implementation of the pertinent provisions, but also to other differences between the legal systems involved.

4 An increasingly negative feature is a deficit in terms of flexibility and balancing ability. On the one hand, *the free flow of data* at EU level is *not to be obstructed*; while, on the other hand, the principle of prohibition continues to enjoy top priority, despite the fact that in the private sphere the freedom of economic activity as well as the freedoms of opinion, expression, information and communications need to be accorded the same priority.

5 As a result, both the EU and each of its member states are bound to define very far-reaching exemptions, so as not to (excessively) impede "normal data processing" and "normal communications". What is lacking is a more explicit substantive definition of the actual object of protection [Schutzgut]. Even the EU Charter of Fundamental Rights refers to the individual and/or the right of personality only in indirect terms while putting the focus on data.

6 The current standardisation of data protection law neither reflects what has meanwhile become standard practice, as very graphically illustrated by Facebook, Google etc., nor technological developments, nor, in particular, the needs of the economy or people's changing communication habits.

7 Particularly ignored is the fact that individuals, in many respects, have become active members of networks in a form that turns them into data processors themselves.[4]

8 Another perception is that, up until now, liability concepts have not been really effective in combating data breaches. Rather, infringements of data protection law have so far been "worthwhile" for the infringers.

9 A special problem is the protection of data in big international corporations in the area of order data processing. Another serious defect of data protection law is the fact that the actual protective mechanisms are overlaid by very vague but high-ranking protection principles, such as the principle of prohibition and the principle of data avoidance.

10 A principle that requires far greater emphasis is the principle of earmarking.

11 The EU currently plans to renew data protection - not, however, by directly amending the EU data protection directive 95/46/EC, but rather, it appears, in the form of a regulation (see GDD [Society for Data Protection and Data Security] press release of 17 November 2011). Some input and public statements by Commissioner Reding[5] are available in advance of this new regulation. Particularly noteworthy in this context is the Commission's legislatory framework of 4 November 2010, laying special emphasis on "privacy by design" and "privacy by default", but also on "accountability" as contemplated new principles to govern a modern form of data protection.[6]

12 The authors have on the one hand sought to present a draft BDSG for the non-public sphere (i.e. the economic field), designed to avoid a substantial number of the "defects" marring the current provisions; while, on the other hand, addressing proposals of the Commission.

13 What can possibly also be achieved by fleshing out a protected interest in terms of substantive law is a larger measure of compatibility with US data protection law. In the US, data protection is largely governed by individual laws while seeking, to a greater extent than in Europe, to strike a balance with the freedom of communication. The concept proposed by the present authors also places greater emphasis on the pursuit of such a balance, by making the protected interest suitable for involvement in a direct balancing process. According to the current regulations, such a balancing process must be implemented at a stage which is not suited to the purpose.

B. The authors' concern

14 The authors have put up for discussion a draft for the renewal of the data protection law.[7] In doing so, they have been guided by the desire to leave well-trodden paths in the assessment and discussion of data protection, pursue new approaches and thereby draw the appropriate consequences.

15 There is general agreement that data protection has to cope with a host of new challenges which, while only being alluded to in manifestations and/or trends reflected in catchwords like "social networks", very often harbour fundamental technological and social changes or possibly even revolutions. Some of these developments have been closely watched and put up for discussion by the EU e.g. through the "Group of 29" or the International Working Group.[8] Thus, the "Group of 29" dealt with the RFID[9] issue, with smart metering[10] and geolocation[11] while social networks were addressed as early as 2009.[12]

16 We propose to show in the context of the following the policy decisions the EU is facing in tackling the planned re-design of European data protection law.[13]

C. Privacy by design

17 First thesis: Privacy by Design is inconceivable and bound to remain a hollow term so long as the focus of protection is on data. Privacy by Design requires modelling and implementation of the Private Sphere as the essential protected legal interest. Otherwise the decisive design standard – also required for purposes of justifiability – would be lacking.

18 The postulate underlying Privacy by Design is to rethink the technological side of the entire data protection regime (including along the lines of privacy-enhancing technologies, PET[14]). What is also needed, however, is bringing into focus the protection of the private sphere as the actual centrepiece of data protection. Privacy by Design is of outstanding importance to the Commission.[15]

19 It is one of the special challenges to define an internationally comprehensible protected legal interest that builds on the protection of the personality, its roles and spheres while departing from the focus on "data" as the primary regulatory purpose. Given the current scope of data processing operations, the aim cannot be to minimise the incidence and usage of data as such without differentiating between different data categories. Rather, any approach along the lines of Privacy by Design must focus on designing technological processes in such a way that the private sphere of users is respected and/or protected to the greatest extent possible.

20 It will hardly be possible to develop appropriate modelling standards for information systems/networks, let alone practicable, deterrent liability concepts **without defining a flexible substantive protected legal interest** (supported by PET[16]). The EU made it clear, already in its Data Protection Directive that data protection should not and must not lead to an obstruction of "the free flow of data". This means in theory, that what is generally accepted is a kind of unison or parity between data protection on the one hand and the free movement of data on the other.[17] In fact, however, data protection has come to prevail over "the free flow of data", which has remained a hollow term for lack of fleshing out.

D. Abolition of the principle of prohibition

21 Second thesis: The principle of prohibition should be abolished as it amounts, in the conditions of networked communications, to a prohibition of communication that is incompatible with the protection of free communication imperative in an open democratic society.

22 The current principle of prohibition amounts to a regime of exemptions to the rule. Actually, exemptions should be narrowly defined as is the case time and time again in data protection literature.[18] However, any narrow interpretation leads to excessive constraints on free communication.

23 While both Germany and the EU, by embracing the principle of prohibition, have internationally come to be reputed for having created a maximum degree of data protection, it is noticeable that in practice data protection has become riddled with holes or even rendered inappropriate compared to most other recent developments. This is partly due to the way exemptions are regulated and the difficulties in interpreting them. Moreover, individuals increasingly become actors within the social networks and/or information systems, so that the classical idea of a kind of antagonism – i.e. the storage/processing systems on the one hand and those affected by them on the other - is no longer tenable.

24 Pitting "data protection" against "the free flow of data" is no viable weighing model. The idea of the free flow of data is right in that the parties involved in it are the individuals affected on the one hand, and institutions on the other which are in a position to claim rights that are secured by the basic law. This applies to both the freedom of communication and – where business activities are concerned - to entrepreneurial freedom.

25 In order to make the personality with its spheres and functions adequately capable of protection, it first has to be implemented e.g. as a protected model. Every attempt to do so in the context of the term "personal data" has failed. Interestingly, the data movement rules of the EU Directive and of the BDSG entirely even out the grading of sensitivities to the point of eliminating them entirely. By contrast, the BDSG's provisions on "safety" (section 9, technical and organisational measures) call for these rules by the backdoor without providing the addressee with a pertinent standard.

26 **The operation of the principle of prohibition**, which triggers a rigid mechanical effect, has been illustrated by *Peifer*, using the example of the behaviour-oriented user approach.[19]

27 "However, the translation of these constitutional values into data protection law has produced a close-meshed regulatory network which, in the individual case, very quickly leads to the enforcement of a rigid principle of prohibition. This is essentially due to four – selected and by no means exhaustive – factors.[20]

28 In this context Peifer cites the following influences:[21]

- the principle of prohibition as such,
- the broad definition of the term "personal data",
- the lacking effect of a consent procedure (consent as a tool practically being insignificant),
- the excessively broad scope of application of the BDSG.

29 Peifer concludes that data protection law is a "prohibition-oriented and rigid instrument".[22]

30 Only very few of the host of tools provided for by the EU Data Protection Directive make a real impact despite the fact that they, unlike the principle of prohibition, are very flexible and far closer to the exercise of control by the personality and/or the individual, in particular through a combination of purpose orientation and earmarking. Within certain limits, the principle of prohibition can in the final analysis be shifted to subsequent stages and/or to the protection of certain spheres, i.e. privacy[23] and/or to the core area of personality.[24] Guiding principles should be freedom of communication combined with disclosure obligations, voluntary commitment[25] and earmarking.

E. Stages of sensitivity and tools, earmarking

31 Third thesis: The protection of the personality can be substantially specified by combining a grading of a basically free movement of data with a staggering of a set of tools, ranging from opting out e.g. in case of a change of earmarking up to opting in and/or requiring consent for the handling of sensitive data because thus a correlation can be established between the intensity of and the need for protection. This enhances the effect of the instrument of earmarking while relegating the principle of prohibition to specific spheres, areas and threats.

32 **"*Earmarking*"** is in theory a high-priority tool in both the BDSG and the EU Directive (see article 6 paras. 1 b) and c). While forming part of the principles of quality in the context of the EU Directive, this instrument makes hardly any impact in practice or is completely absent there. Given that you cannot, for lack of context, recognise the sensitivity or triviality of data as such, it is imperative to introduce the context factor for purposes of protection and, consequently, roles and spheres. This is a matter of the self-monitoring of selective and/or sectoral visibility.

33 The voluntary nature of participation in (Internet-based) communication must not lead to an unbridled obligatory surrender of the resultant data. This applies notwithstanding the fact that "data" has long since become a form of currency.[26] The barter trade is taking place in terms of commercialisation[27] where the party affected surrenders "its" data against gratuitous performances. Seen from this angle, many large providers offering services without direct payment are acting as "data hoovers" bent on cashing in on their success reflected in the large number of participants through the sale of and/or trade in the data thus collected.[28] What is required in regard to this kind of data is a limitation of usability by earmarking.

34 Where potential protection is concerned, what matters is not more or less conscious statements (externalism), but rather their perpetuation and alternative use (misappropriation). What still needs to grow is the awareness that "communication data" – at least in the non-contractual context – is primarily intended only for the area of communications and may not, where appropriate, be used in a cursory manner. The "traces" of communications on the net, call to mind that a laptop is not a fall-back position, but nevertheless belongs to the private sphere and is subject to the protection of secrecy.[29]

35 A multi-stage system[30] could cover a spectrum ranging from:

1. Freedom of information and (online) freedom of action
2. through earmarking,
3. limited, sectoral visibility,
4. specific areas, types of data/conditions up to
5. prohibition in principle complete with protection of the core of personality.

36 Until now the "special categories of data" (article 8 EU Directive) have been a foreign body in the regulatory system since neither the EU Directive nor the BDSG is based on a substantive law concept embracing the spheres and/or roles of the individual and the varying "sensitivities" and visibilities involved. This is where clear priorities should be established along with a system of distinct differentiation between diverse stages of sensitivity.

F. Balancing capacity of the protection model

37 Fourth thesis: Art. 8 of the EU Charter of Fundamental Rights ranks the protection of personal data among the fundamental rights. This does not by any means establish prohibition as a sacrosanct prin-

ciple. Article 11 of the Charter of Fundamental Rights (freedom of expression and information) lays claim to the same priority as article 8, so that there is no way of postulating the precedence of one of these fundamental rights over the other. Statements covered by the protection of article 11 are in any event "legitimate" pursuant to article 8.

38 Hence, making a general rule for the handling of personal information – i.e. a rule not confined to the principle of prohibition – would be compatible with article 8 of the Charter provided that, in lieu of that principle, a balancing level were introduced, pitting the protection of the individual against the freedom of information, communication and expression. In that case, the handling of personal information would be directly governed by the principle of good faith even though various substantive counter-positions of the data processor would also be taken into account.

39 The present thesis therefore needs to be supplemented by the sub-thesis that the actual obstacle to adjusting to a substantive protected legal interest is not the Charter but rather the EU Data Protection Directive. After all, article 7 of EU Directive 95/46 makes it abundantly clear, even though not by the same terms, that personal data may be processed "only" if one of the requirements listed in the Directive is satisfied. The following listing is enumerative, only offering rudimentary balancing opportunities while specifying another extremely powerful data protection tool, i.e. the *principle of necessity* (in sub-para. c).

40 Article 7 would have to be modified if the protection of personal data were to be replaced by the substantive protection of the personality from being impaired by the processing of information by weighing such protection against the justified interests of the party processing such information. A pertinent key is provided by article 9 in regard to freedom of expression. Given, however, that the other rights of data processors would have to be taken into account at almost the same ranking, care needs to be taken of a plethora of further equally fundamental rights. It appears appropriate to abolish the principle of prohibition rather than to first establish the ban and then follow it up with a host of further exemptions.

G. Transparency to counter an intangible threat

41 Fifth thesis: Transparency means for the individual to be aware of the threat potential arising in the wake the "data traces"[31] left behind and accumulating – mostly as a matter of course. One possible approach is the principle of "accountability".[32]

42 The "diffusely perceived" threat has relevance in terms of constitutional law.[33] The BVerfG (Federal Constitutional Court), as early as in its ruling on the census, affirmed the existence of inter-action between the fear of expressing one's opinion – i.e. a phenomenon to be taken into account very carefully from the point of view of democracy – and the consequent constraint and risk of being observed.[34]

43 While the BDSG is being interpreted as establishing a right to informational self-determination – even as a protected legal interest.[35] The legislator has not acted on it, not even in section 1 para. 1 ("Object") even though there is no unintentional lacuna because the mandate to incorporate this legal tenet was deliberately omitted by several amendments. Meanwhile, the same applies to the fundamental IT right (fundamental right to safeguarding the integrity and confidentiality of information technology systems) which was not expressly incorporated either.[36] In view of the three amendments made in 2009[37] this omission is not due to oversight.

44 Arguing for the need to incorporate the fundamental IT right, the BVerfG expressly points to lacunae in the scope of protection offered by the right to informational self-determination.[38] In response to new threats, the BVerfG has again broadened the range of protected legal interests, specifically by adding the IT systems of the fundamental rights holder. The right to privacy encompasses this fundamental right by way of protection against "secret" infiltration, expressly protecting the "core area of the personal way of life".[39] What is therefore called for now is a re-definition of the protected legal interest including provision for diverse spheres of visibility and sensitivity.

45 Logging of user behaviour is tantamount to spying them out. Secret spying out is perceived as interference with the private sphere even if conducted entirely anonymously.[40]

46 The secrecy of observation has a clear parallel in the internet user profile. Many users perceive the wide-ranging storing of data at Facebook, Apple and Google as interference with their private sphere. The secret and uncontrolled logging and evaluation of user habits is perceived as spy-out of the user differing but slightly, if at all, from the targeted online search of a computer hard disc.

47 The BVerfG has addressed the "diffuse menace" inherent in the logging of user behaviour. While the court's ruling relates to public authorities,[41] the menace also emanates from "*Facebook*", "*Apple*" or "*Google*", and/or users perceive a "diffuse threat" from the "traces" left by them on the Net.[42]

48 The BVerfG demands transparency to counter the "diffuse threat" posed by uncontrolled data stocks, which permits the conclusion that the legislator is called upon to create clear-cut regulations for the collection and usage of data stocks.[43]

49 The burden weighing on the individual[44] in the form of data relating to him/her as a concrete embodiment of "threat", i.e. the actual potential, could substantially be reduced if "cursory" traces of and, in particular, "waste products" from the use of technological systems were to remain cursory, i.e. fade at short notice and thereafter disappear, also against the background of the "right to oblivion".[45]

50 **The requirement enshrined in constitutional law is a ban at least on "total data capture" by the state.**[46] This must also apply to the non-public sector. The danger arises where earmarking in combination with merely sectoral visibility is not complied with.[47]

51 "Thus, the introduction of telecommunications data storage cannot be looked upon as a model for the creation of further collections of groundlessly retained data, but rather compels the legislator to observe greater restraint when considering new storage obligations or authorisations against the background of the entirety of already existing data pools. The fact that the exercise of freedom by citizens must not be totally recorded and registered forms part of the constitutional identity of the Federal Republic of Germany (cf. the BVerfG on the reservation of identity as enshrined in the Basic Law, ruling of the Second Senate dated 30/6/2009 – 2 BvE 2/08 et al. – juris, marginal no. 240) to the protection of which the Federal Republic is committed both in a European and an international context. The precautionary retention of telecommunications data considerably narrows the leeway for further groundless data collections including through the European Union."[48]

52 What is required is a kind of amendment to the right to integrity of the private "ITC sphere", possibly along the lines of the BVerfG's judgment on online search[49] - a ruling also taken up by the Commission.[50]

53 "The general right to privacy (article 2 para. 1 in conjunction with article 1 para. 1 Basic Law) encompasses the fundamental right to guarantee of the confidentiality and integrity of information technology systems."

54 The amendment would be to the effect that such prohibition in principle must not be confined to the secret spying out of the private ITC but must extend to the indirect use thereof through deep packet inspection or through the environment of application programmes and/or the browser (e.g. via flash cookies).

H. Strengthening of the requirement of consent as a tool

55 Sixth thesis: The usability of **consent** is being overestimated.

56 Consent is not seen, at least in Germany, as a viable alternative to a legal reform as a basis.

57 While theory looks upon consent as the best means of ensuring the autonomy of the parties affected, it proves inappropriate in the concrete conditions prevailing. The pertinent requirements of the EU Directive, which in view of the mass traffic on the Internet necessarily demand standardised, pre-formulated declarations of consent, can hardly be satisfied ("without any duress, case-specific and in awareness of the factual situation", art. 2 h).

58 While court practice has charted suitable ways of drawing up consent clauses that are "watertight" for the purposes of general terms and conditions, the effectiveness of a consent is jeopardised, even as an individual declaration, if it is too global (not sufficiently specific) or if it relates – entirely or partly – to a form of collection, storage and use of data that is permissible under a legal provision (such as section 28 BDSG).

59 The relationship between consent and a (legitimising) legal provision is by no means clear or simple. The generally accepted view appears to be that consent is not to be and cannot effectively be procured, where a different standard of consent is already applicable.[51] It is not clear what is still expected in terms of legal consequences if the consent of the data subject is – ineffectively – additionally procured for a form of data processing permitted by law. *Sokol* advises against procuring consent merely for reasons of "legal security".[52] The data subject was likely to jump to the conclusion "*that he/she had a choice including the option of refusing the contemplated form of data use*".[53] Unlike this, the requirement of consent might be recommendable despite the parallel existence of a statutory regime of consent "*where public authorities or enterprises ... are prepared to respect the refusal of consent by the person concerned*".[54]

60 However, this view would leave **no room** for consent in a situation where processing **obligations** are imposed by law.[55] Considerable uncertainties would arise in cases requiring a careful distinction between processing obligations on the one hand and processing rights on the other, so that enterprises would

have to weigh one choice against the other in cases where the two options are very similar.

61 A concept of stages would clearly be the better choice when it comes to effectively procuring consents and being able to rely on their unassailability.

I. Combination of liability concept and security requirements

62 Seventh thesis**:** Data protection would be strengthened by a combination of liability without fault, compensation also for non-material damage and the duty to design ITC systems in a privacy-oriented manner complete with the security of these systems. Here is a concrete proposal on this point, patterned on article 17 of the EU Directive and section 3 a p. 1 of the BDSG, with special reference to the latter's approach concerning the design of ITC systems.

63 What is needed is to combine the personality and earmarking oriented design of information systems with the pertinent security requirements in such a manner that any design jeopardising the personality already amounts to a data breach.[56] To achieve this, data processing and information systems need to be designed in a way that corresponds to the characteristics of the personality and, in particular, to a kind of visibility that is geared to specific purposes, and in a way that affords the protection of differentiated spheres.[57]

64 Proposal:[58]

....

Section 6 Damages

(1) A data processor injuring the data subject by a form of collection, processing, transmission or use of personal information that is inadmissible or incorrect under this law shall be liable for damages to such data subject. This liability shall lapse where the data processor proves that he/she has complied with his/her obligation to proceed in accordance with the requirements of data protection (section 7 para. 1 second sentence)

(2) Where a data processor infringes the prohibition imposed by section 5 para. 2 [prohibition of the transmission of personal information] section 97 para. 2 second and third sentences UrhG (Copyright Act) shall analogously apply in determining the level of damages.

(3) The data subject shall be entitled to monetary compensation also if the damage does not involve a financial loss provided that this is just and fair under the circumstances.

Section 7 Fleshing out of the procedures

(1) In developing, fleshing out, changing or broadening the procedures a data processor is using or wishes to use, he/she shall at each stage be mindful of the risk of personality rights being jeopardised if personal information is collected, processed, transmitted or used. The processor is therefore obliged to comply with the following guidelines to the extent that this is possible in view of the intended purpose, and that the time and effort involved are not disproportionate to the contemplated purpose of protection.

(2) Procedures shall be geared to the objective of limiting the collection, processing and use of information to the minimum.

(3) Procedures are to be so designed that personal information is automatically erased if and when it is no longer required for the intended purpose unless this is opposed by statutory preservation obligations. Archiving and use for the exclusive purpose of preserving evidence is permissible.

(4) The reliability of the procedures shall be geared at the state of technology. In particular, the state of technology shall be observed in protecting personal information against unauthorised third-party access.

65 In addition, there are strong arguments in favour of liability for the accuracy and completeness of information on the understanding that provision could be made for compensation without fault for **non-material** damage. This may be complemented by counter-statement rights and an automatic duty of notification along with liability for failure to do so ("Skandalisierungspflicht").[59]

Endnotes

1 The first national data protection act. The principle of transparency is much older in Sweden (enshrined in the constitution since 1766).

2 Proclaimed on 1 February, 1977, BGBl (Federal Law Gazette) I. p. 201, fully entered into force on 1 January 1979.

3 The oldest data protection act, albeit limited to one Federal State. Entered into force on 13 October 1970.

4 To some extent recognisable also in assessment platforms, see on this point BGH dated 23 June 2009 –VI ZR 196/08 - spickmich.

5 See also *Reding*, ZD 2011, 1.

6 See also: On the demand for adjustment to the level of technological development -Resolution of the Conference of Data Protection Commissioners of the Federal Republic and the Federal States, 78th Conference 8 and 9 October 2009.

7 Published under www.schneider-haerting.de; see also *Schneider/Härting,* Why we need a new BDSG (Federal Data Protection Law), ZD 2011, 63

8 E.g. on event recorders: Working Paper No. 645.42.10 dated 4/4/2011.

9 Opinion 9/2011 on the revised industry proposal for a privacy and data protection impact assessment framework for RFID applications, 11/2/2011, Working Paper 180.

10 Opinion 12/2011 on smart metering, 4/4/2011, Working Paper 183.

11 Opinion 13/2011 on geolocation services on smart mobile devices, 16/5/2011, Working Paper 185.

12 See Opinion 5/2009 on online social networking, 12/6/2009, Working Paper 163.

13 See Framework Concept of the EU Commission dated 4/11/2010, KOM (2010) 609 final.

14 See on this subject: *Hornung,* ZD 2011, 51 including further quotations; see also: Study on the economic benefits of privacy enhancing technologies (PETs), Final Report to the European Commission, July 2010.

15 See *Reding,* ZD 2011, 1; EU Commission dated 4/11/2010, KOM (2010) 609 final.

16 See *Hornung*, ZD 2011, 51 including further quotations.

17 See e.g. Article 1 para. 2 Dir. 95/46/EC: Member States shall neither restrict nor prohibit the free flow of personal data.

18 See e.g. *Simitis* in: Simitis, BDSG, 7th printing 2011, marginal no. 54 et seq. concerning admissibility alternatives in section 28; more on this issue also below under 7.

19 *Peifer, K&R 2011, 543*

20 *Peifer, K&R 2011, 543,544 including further quotations.*

21 *Peifer, K&R 2011, 543,544.*

22 Peifer, K&R 2011, 543, 547.

23 *On the determination of classification and boundaries in the context of a sexual offence see e.g. BVerfG (Federal Constitutional Court) dated 10/6/2009 – BvR 1107/09, MMR 2009/693.*

24 See BVerfG dated 3/3/2004 -1 BvR 2378/98 et al. – Eavesdropping attack, CR 2004, 343.

25 See also *Härting/Schneider*, ZD 2011, 63; dies., ZRP 2011, vol. 8 (i.E.).

26 Cf. Ilse Aigner "Facebook makes use of personal data as a currency", FOCUS Online, Saturday, 17/7/2010, 11:15; Matthias Schrader, "Data are the petroleum of the future", FOCUS Online, Thursday, 12/5/2011, 12:29.

27 *Weichert*, The economisation of the right to informational self-determination, NJW 2001, 1463.

28 See also on the business model – even if without in-depth economic expertise and highly populist approach -*Kurz/Rieger*, The data eaters, Frankfurt 2011.

29 See *Heckmann,* Public Privacy – protection of the weaker on the Internet, K&R 2010, 1463.

30 See also *Schneider,* AnwBl. 2011, 233, 237 et seq.

31 See already *Köhntopp/Köhntopp*, CR 2000, 248, 250 et seq.

32 See also Group of 29, Opinion 3/2010 on the principle of accountability, 13 July 2010, Working Paper 173; EU Commission dated 4/11/2010, KOM (2010) 609 final,

33 See on the following also *Härting/Schneider*, ZRP 2011, p. 233.

34 From the point of view of a state governed by the rule of law and of democracy, the right to informational self-determination therefore is the proper answer: BVerfG dated 25/12/1983 – 1 BvR 209 et al. BVerfGE 65, 1 – Census.

35 See especially Simitis, in: Simitis (publisher), BDSG Commentary, 7th printing, section 1 marginal no. 23 et seq.; see also on this subject *Schneider/Härting*, ZD 2011, 63, 64.

36 BVerfG dated 27/2/2008 – 1 BvR 370/07 et al., NJW 2008, 822 et seq. – Online search; see on this subject *Luch*, MMR 2011, 75 et seq..; *Baum*, DuD 2011, 595.

37 See e.g. *Drewes*, CR 2010, 759 on the List privilege, *Brink/Schmidt*, MMR 2010, 592 on staff screening, on this subject also *Bierekoven*, CR 2010, 203; see also *Hanloser*, MMR 2009, 594 (on amendment II).

38 BVerfG dated 27/2/2008 – 1 BvR 370/07 et al., NJW 2008, 822, 824 – Online search

39 BVerfG dated 27/2/2008 – 1 BvR 370/07 et al., NJW 2008, 822, 826 – Online search

40 *Härting*, Internet law, 4th Ed., 2010, marginal no. 72.

41 BVerfG date 2//.2010 – 1 BvR 256/08 et al., NJW 2010, 833, 843 – data retention.

42 *Härting*, AnwBl., 2011, 246, 247.

43 Cf. *Hoffmann-Riem*, JZ 2008, 1009, 1010 et seq.

44 It would be highly important to "measure" the overall impact, see on (the unlawful) "cumulative effect", *Knierim*, ZD 2011, 17 including further quotations

45 S.a. *Reding*, ZD 2011, 1, 2.

46 For examination, but there still answered in the negative, see BVerfG dated 2/3/2010 – 1 BvR 256/08 et al. – Data retention, NJW 2010, 833, marginal no. 216, including cross reference to BVerfG date 30/6/2009 – 2 BvE 2/08 et al. in marginal no. 218, immediately followed by the quotation.

47 See also: *Schneider*, AnwBl 2011, 233, 236 et seq.

48 BVerfG dated 2/3/2010 – 1 BvR 256/08 et al. – Data retention, NJW 2010, 833, marginal no. 218

49 See on this ruling e.g. *Luch,* Das neue "IT-Grundrecht" (The New Fundamental IT Right). Grundbedingungen einer "Online-Handlungsfreiheit" (Basic prerequisites of an online freedom of action) , MMR 2011, 75; *Bär*, MMR 2008, 315.

50 EC-Commission dated 4/11/2010, COM (2010) 609 final, 2.1.1, footnote 14.

51 Gola/Schomerus, BDSG, section 4 marginal no. 16; *Taeger* in Taeger/Gabel, BDSG, section 4 marginal no. 47.

52 *Sokol* in Simitis, BDSG, 7th printing 2011, section 4, marginal no. 6.

53 *Sokol* in Simitis, loc. cit. marginal no. 4.

54 *Sokol* in Simitis, loc. cit. marginal no. 6; cf. also *Simitis* in Simitis, BDSG, 7th printing 2011, section 28, marginal no. 20.

55 *Sokol* in Simitis, loc. cit., marginal no. 7.

56 See also *Schneider*, ZD 2011, 6.

57 See also Schneider, AnwBl 2011, 233.

58 See also www.schneider-haerting.de.

59 See on 42a BDSG, "Data Breach" *Karger*, ITRB 2010, 161; *Dix* in Simitis, BDSG, 7th printing 2011, marginal no. 1 concerning the contribution to transparency and marginal no. 2 concerning the scope of application. The latter still appears to be too narrow. On the intra-company resolution of the conflict with "Compliance" see *Hamm*, NJW 2010, 1332.