Convenience translation of

THOMAS KRANIG / STEFAN PEINTINGER, Selbstregulierung im Datenschutzrecht, ZD 2014, 3ff.

by Thomas Kranig and Stefan Peintinger*

Self-regulation with regard to Data Protection Law

by Thomas Kranig and Stefan Peintinger*

Legal aspects of self-regulation with regard to Germany, Europe and the US in due consideration of the proposal for an European General Data Protection Regulation (GDPR)

I. Introduction

This article shall provide an overview of the legal instrument "self-regulation" with regard to Data Protection Law in Germany and Europe as well as with regard to Information Privacy Law in the US. In the US self-regulation is a very important tool. However, in Germany and Europe (hereinafter: "here") it is almost insignificant. This article is dealing with the question why this legal instrument here is not commonly used. Furthermore, the authors explore if self-regulation will take on greater significance with regard to the proposed Art. 38 GDPR[1] by the *European Commission*.

There are significant differences between the German and European Data Protection Law and the corresponding US law on Information Privacy. Here, the basic approach to processing personal data is "reservation of authorization" either by law or by consent of the data subject. In the US, processing of personal data is generally allowed if it is not prohibited by law. In addition to these different points of view, there are comparable legal instruments. One of them is self-regulation with regard to Data Protection Law, respectively, Information Privacy Law (hereinafter: "Privacy Law"). This principle was identified as a guideline with regard to Privacy Law by the *Organisation for Economic Co-operation and Development (OECD)*.[2]

II. German and European point of view

1. Introduction

In accordance with Art. 27 (1) Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)[3] Member States and the *European Commission* encourage the drawing up of codes of conduct, intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to the Data Protection Directive, taking into account the specific features of the various sectors. This wording indicates that from a European point of view on Privacy Law, a code of conduct can only address the implementation of data protection provisions. A code of conduct may not be used, under no circumstance, to replace data protection provisions or to establish a legal basis for authorization purposes. The German Federal Data Protection Act (BDSG) has implemented Art. 27 Data Protection Directive through Sec. 38 a BDSG. Both regulations are comparable with regard to the wording and they are both (only) dealing with the implementation of data protection provisions.

Here the term "controlled"[4] or "regulated"[5] self-regulation (or commitment) is used. This means that associations and other entities which represent specific groups of controllers may draft codes of conduct with regard to Privacy Law self-regulation. These codes of conduct can address characteristic

features of a specific industry and they should provide a practical solution for various aspects on the implementation of Privacy Law. There is no specification with regard to the extent of these codes of conduct. It is possible just to address one specific topic of processing personal data. Therefore, it is possible to respond to specific business needs[6] and a practical technical solution can be developed.[7] Furthermore, via this process, a code of conduct, as an interpretation of data protection provisions, can be developed, which is authorized by the relevant (state) supervisory authority.[8] Therefore legal uncertainties and disputes can be avoided. The drafted proposal is then submitted to the supervisory authority which examine the compatibility of the submitted drafts with the applicable law on data protection.

The wording of Sec. 38 a (1) BDSG requires the "draft rules of conduct to promote the implementation of data protection provisions". Today, there is no dispute among the different supervisory authorities anymore with regard to the meaning of "promote". A former legal opinion asked for an increased standard, i.e. a stricter standard, on Privacy Law, compared to the relevant legal provisions.[9] Today, in contrast, supervisory authorities only ask for a substantiation of undefined legal terms and/or with regard to guidelines for exercising discretion.[10] Under no circumstances may a code of conduct fall below Privacy Law standards set out by relevant legal provisions. If the supervisory authority asserts that the drafted code of conduct is promoting the implementation of data protection provisions, an administrative act which results in a benefit is issued, determining this finding.[11] Therefore this process is called "controlled" or "regulated" self-regulation.

There are various arguments against this form of self-regulation. Business stakeholders argue that by implementing a code of conduct two regimes are established to follow along. Therefore, the risk of violation unfair competition laws increases. While drafting such a code of conduct it is difficult to balance different interests such as the right of self-determination by the data subject and the legitimate interest of each business (even with respect to other businesses within an association).[12] Furthermore, businesses argue that there are no practical incentives and the implementation is not supervised in a sufficient manner.[13] In addition, the costs of this proceeding and the costs of managing these aspects of Privacy Law are too high, especially for small and medium enterprises.[14] It seems unlikely that the argument prevails that there is a risk to avoid legislative processes via self-regulation.[15] Self-regulation may only be used within a narrow scope. However, self-regulation cannot be taken for granted.

2. Examples

In 2001, § 38 a BDSG came into effect. Apparently only one code of conduct, by the "*Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV)*", was examined as being in accordance with the applicable law on data protection, § 38 a (2) BDSG. The examination was conducted by the supervisory authority of the "Stadtstaat" Berlin. This administrative act (which results in a benefit) was issued after every other (state) supervisory authority had agreed on the result within the framework of the so called "*Düsseldorfer Kreis*".[16] By agreeing on the result, a self-commitment came to pass by these other (state) supervisory authorities. Therefore, the "*Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft (Code of Conduct)*", dated 7th of September 2012,[17] are in accordance with data protection provisions. These principles do not establish stricter regulations by the insurance sector for processing personal data, however, they clarify the scope of consent and the release from certain non-disclosure obligations. Certain legal requirements are substantiated for this sector and therefore these legal requirements are easier to follow along from a practical point of view. Therefore, this code of conduct is very significant to all stakeholders. However, this code of conduct is (unfortunately) the only example of a successful self-regulation in accordance with § 38 a BDSG in Germany.

Other examples of "self-regulation", which were not examined in accordance with § 38 a BDSG, are: "*Datenschutz-Kodex für Geodatendienste*",[18] the "*Datenschutz-Kodex für soziale Netzwerke*"[19] and different codes of conduct by the "*Deutscher Dialogmarketing Verband e.V.*".[20] Furthermore "self-regulation" is used with regard to market and social research[21] and with regard to the so called "*Robinson list*".[22]

On the European level, there is the "*European Code of Practice for the use of personal data in direct marketing*" by the *Federation of European Direct Marketing*.[23] This code defines various terminologies and sets out certain scenarios of data processing.[24]

3. Legal nature of self-regulation in Germany

Self-regulation is a legal instrument sui generis. Parties are bound by the administrative act. The relevant (state) supervisory authority cannot argue after the acceptance of a self-regulation concept that this code of conduct is not in accordance with data protection provisions. In order to withdraw or to revoke the administrative act which resulted in a benefit, the supervisory authority has to act in accordance with §§ 48 or 49 VwVfG (German Administrative Procedure Act). However, the supervisory authority may determine that the implantation itself of this self-regulation is not sufficient, i.e. not promoting the implementation of data protection provisions in accordance with § 38 a BDSG. Furthermore, a code of conduct does not release someone from acting in accordance with data protection provisions. Self-regulation should only help applying data protection provisions but it should not set aside or change the meaning of data protection provisions.[25]

If an association is operating within the whole Federal Republic of Germany, i.e. not only within one Federal State, and if the code of conduct by this association is determined as being in accordance with § 38 a BDSG by the relevant supervisory authority, this decision is binding with regard to the matters of fact. Furthermore, with regard to the only case at hand, the other supervisory authorities followed this administrative decision after discussing it within the so called "*Düsseldorfer Kreis*". This harmonized legal assessment is helping to promote the acceptance of an administrative decision with regard to § 38 a BDSG.

The approved code of conduct is not automatically legally binding for every member of an association.[26] In fact, every association has to deal with the implementation and enforcement of such a code of conduct by itself. Besides an explicit contract, this can be achieved by the general terms and conditions of this association or via general terms and conditions by every single member. Furthermore, the existence of a code of conduct may be relevant with regard to §§ 1 ff UWG (German Act Against Unfair Competition).[27]

4. Enforcement

Even though only parties involved in an administrative proceeding can be bound by an administrative act, concluding such a proceeding, a code of conduct may be of greater importance to other third party proceedings. If a third party is processing personal data in a comparable fashion, the supervisory authority considering its previous administrative act will act. Therefore a legal standard can be set, which can be used for orientation purposes by third parties as well. In addition, if an administrative act is challenged in front of an administrative court, this court needs to consider the code of conduct as well when reviewing the exercising of discretion by a supervisory authority.

II. US point of view

1. Introduction

In the US there is no comprehensive Privacy Law.[28] Privacy Law regulations are rather implemented in response to specific situations, such as the „Video Privacy Protection Act" (1998), the „Fair Credit Reporting Act" (1971) or the „Children Online Privacy Protection Act" (COPPA; 1998). COPPA was reformed with effect from July 1, 2013.[29] Therefore it is not true to state that there is no Privacy Law at all in the US.[30]

US legal tradition is regarding self-regulation as an effective approach in order to achieve tailored solutions.[31] This tool is supposed to ensure a detailed balance between different stakeholders. Furthermore, US Privacy Law is much more driven by aspects of competition, i.e. aspects of supply and demand. In comparison, in Europe and Germany Privacy Law is seen as a fundamental right of every person and not as a result of competition.[32] Therefore it is reasonable to believe that if existing or potential costumers would like to have "more" privacy protection, they would contract with a respected provider. In general, it seems that there is a fear, Privacy Law (in terms of an European approach) would hinder innovation.

Self-regulation is seen as a key to provide flexible regimes.[33] In the US, as well as in Germany,[34] self-regulation with regard to Privacy Law is compared to self-regulation with regard to Environmental Law.[35] In the context of Environmental Law, "one size fits all" and "top down" approaches have been replaced respectively amended by the instrument of self-regulation ("bottom up").

In the US self-regulation cannot just be used by certain qualified associations. Any person or entity collecting, processing or using personal data on his or its own behalf or commissioning others to do the same may use this tool. In general, there is no process to assess a self-regulation concept by a supervisory authority before the beginning of data processing. To the extent evident, only COPPA provides for the *Federal Trade Commission* (*FTC*) to evaluate a self-regulation concept by "industry groups or other persons".[36]

There are arguments against self-regulation in the US as well. Guiding principles of Privacy Law are only implemented in a weak fashion or not at all. There are no incentives for a single sector-wide self-regulation approach. Compliance with self-regulation is in certain cases inefficient and in general there is a lack of transparency.[37] As an example, this lack of transparency is a result of insufficient clarification on how personal data is used to begin with.[38] Furthermore, critics argue that self-regulation is often used to avoid the enactment of State or Federal Privacy Laws.[39] Therefore, some US commentators demand a coexistence between self-regulation and (more) legislative measures by State and/or Federal Authorities, respectively a more "regulated" approach to self-regulation.[40]

In the context of the publishing "*Consumer Data Privacy in a Networked World*" by the *White House* on February 23, 2013,[41] the interaction of self-regulation and the enforcement of Privacy Laws by State and Federal authorities is emphasized as well.[42] Among other proposals, it is intended to provide incentives for companies to adopt an enforceable code of conduct. The *FTC* should advise on procedural questions as well as on subject matters. Complying with such a code of conduct is still voluntary. However, if there is "any investigation or enforcement action related to the subject matter of one or more codes, the *FTC* should consider the company's adherence to the codes favorably."[43]

In conclusion, the scope of self-regulation is very wide in the US. "Privacy Statements" or "Privacy Policies" are already regarded as a type of self-regulation.

2. Examples

One US example for self-regulation is the processing of personal information of children under the age of thirteen. If a company is complying with certain rules via a code of conduct, it is supposedly acting

within the COPPA framework.[44] The principles of the "*Children's Advertising Review Unit*" (*CARU*) are one example of an approved code of conduct with regard to COPPA.[45] There are various "core principles" laid out, such as taking into account the limited knowledge, experience, sophistication and maturity of the audience to which the message is directed. Furthermore, advertising should be neither deceptive nor unfair, as these terms are applied under the FTC Act, to the children to whom it is directed.[46]

Further examples are:[47] "*Privacy Promise of the Direct Marketing Association (DMA)*",[48] the *"Network Advertising Initiative (NAI) Principles*"[49] and so called "privacy seal programs", i.e. private companies issuing certain certifications, *TRUSTe*,[50] *BBBOnline*[51] as well as the "*Online Privacy Alliance (OPA) Guidelines*".[52] In the past, there were the so called "*Individual Reference Service Group (IRSG) Principles*", too.[53]

Additionally, in the US the so called "*Safe Harbor Principles*"[54] are seen as a form of self-regulation as well.[55] First and foremost, the Safe Harbor Framework is an agreement between the *EU Commission* and the *US government*, represented by the *US Department of Commerce*.[56] Through the Safe Harbor Framework a regulated concept of self-regulation was established in the US. This is the legal basis for transferring personal data to the US, being a third country in accordance with Art. 25 Data Protection Directive.[57] US companies may voluntarily agree on adopting the Safe Harbor principles. They have to indicate this to the *US Department of Commerce* and afterwards their name is published. Thereby these codes of conduct become mandatory and these companies can be held accountable.[58] *Taildou* refers to this concept as a compromise between two highly diverse point of views.[59]

3. Legal nature of self-regulation in the US

In the US, self-regulation is a legal instrument sui generis as well. The fact that self-regulation in general is possible is not laid out by a statute. Self-regulations are regarded as emerging norms of regulatory practices. On the one hand, in Germany and Europe self-regulation can only be used in order to address the implementation of data protection provisions.[60] On the other hand, in the US this instrument is often used to avoid federal or state legislation. A company or an association can only accept self-regulation, in general, on a voluntary basis. However, self-regulation is playing a vital role with regard to Privacy Law enforcement by the *FTC*.[61]

4. Enforcement

There is no genuine Privacy Law authority in the US. Therefore, the *FTC* (among other authorities) is dealing with Privacy Law violations with regard to Sec. 5 FTC Act (= 15 Code of Laws of the United States of America (U.S.C.) § 45).[62] The *FTC* is proceeding on the assumption that it is an act of unfair competition with regard to 15 U.S.C. § 45 (a), if a company is publishing a code of conduct, stating that it is following along, and then it does not follow through with this "promise".[63] Furthermore, State Attorney Generals are also playing an important role enforcing Privacy Law in order to protect consumers.[64]

The question on how a code of conduct is implemented within an association is an internal matter of this entity. In addition self-regulation is more important considering protection against unfair competition.

IV. Comparison

1. Introduction

Self-regulation is a good example in order to point out the different approach to Privacy Law in Germany/Europe and the US. The different meaning of self-regulation is due to the difference on the basic approach to Privacy Law.[65] Here, there is an approach to have a complete set of rules governing Privacy Law. In the US – from an European point of view – there is an "island effect" with regard to Privacy Law regulation. Therefore it is understandable that self-regulation is seen as being more important compared to Germany/Europe. The different legal traditions as well as the different basic approaches may be one explanation for the question, why self-regulation is more successful in the US, compared to Germany/Europe.[66] Another piece of the puzzle may be that self-regulation in the US is often regarded as a tool to avoid state or federal legislation.

2. Common features

The advantages of self-regulation may be evident, if the benefits, which can be seen in the US, are carried over to Germany/Europe. Self-regulation helps to avoid legal uncertainties with regard to the application of Privacy Laws. Data processing within an entity can be designed in a way that makes it unnecessary for supervisory authorities to act. By discussing the planned data processing with a relevant authority, a company can clarify the scope at hand before data processing takes place. In the long run, risks associated with data processing can be reduced. Furthermore, by drafting a code of conduct, awareness with regard to Privacy Law can be raised. This might be particularly helpful with regard to current Privacy Law discussions.

3. Differences

One major difference between Germany/Europe and the US is the framework for self-regulation.[67] Here, there is the "reservation of authorization" approach and there are only certain provisions allowing data processing. In the US, in general, each data subject is very much dependent on the wording of a code of conduct. If there is no special regulation and if the code of conduct is not offering remedies, a data subject can only file a complaint with the *FTC* or another relevant authority. From a German/European point of view, it is problematic that data processing in the US is allowed in general, if there is no specific prohibition.[68]

Another difference is the fact that in the US each company can use self-regulation for itself. Here, only certain associations may use this tool because of the wording of Art. 27 (2) Data Protection Directive respectively § 38 a (1) BDSG. Self-regulation is moreover an instrument to avoid US state or federal legislation. For this purpose the "Safe Harbor Principles" are an example. They have been adopted to avoid relevant legislation.[69]

In conclusion, the German word "Selbstregulierung" can be translated as "self-regulation". However, at the moment, these words don't share the identical legal meaning. Here, self-regulation is only allowed with regard to certain aspects of the implementation of data protection provisions. In the US, self-regulation can be used on a wide scope and it is, in general, not approved beforehand by a supervisory authority. In this regard, COPPA provides an exemption. The *FTC*, in general, is only acting ex post in order to regulate competition aspects of Privacy Law violations.

V. Prospected proposal for a General Data Protection Regulation (GDPR)

Self-regulation is not playing a significant role in European legal practice. The discussion with regard to the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), dated January 25, 2012, may offer a chance for a new impulse.[70] Maybe self-regulation might obtain higher acceptance if the framework is set in a practical manner.

1. Codes of Conduct in accordance with the proposed Art. 38 GDPR

The proposed Art. 38 GDPR is based on Art. 27 Data Protection Directive. However, there are significant changes proposed. The basic approach has not changed and the proposed Art. 38 GDPR is dealing with "codes of conduct intended to contribute to the proper application of this Regulation" (see proposed Art. 38 (1) GDPR). However, compared to Art. 27 Data Protection Directive, there are more details with regard to the role of supervisory authorities to encourage the drafting of code of conducts. Furthermore, particular features of a code of conduct are mentioned and more entities are allowed to use self-regulation.

One major change with regard to the current German legal situation is the way of adopting self-regulation in accordance with § 38 a BDSG. In Germany, self-regulation can be put into effect by an administrative act which results in a benefit. Based on the draft GDPR, supervisory authorities only have certain rights with regard to the European administrative proceeding. They can only ask specific questions if the planed self-regulation concept is only targeting the Member State, where this supervisory authority is located. There is no provision on how such a self-regulation is becoming legally binding in one single Member State. § 38 a BDSG might become less important after the adoption of the proposed GDPR and maybe, in the future, there is no discretionary competence by a German supervisory authority. If an entity wants to draft an European-wide code of conduct, the *European Commission* shall be the relevant authority (Art. 38 (3) GDPR). The *European Commission* would be responsible for the general validity of such a code of conduct (Art. 38 (4) GDPR). This form of general validity is, however, only a legally binding Union act and the Member States need to implement such acts, proposed Art. 38 (4), 87, GDPR in accordance with Art. 291 (1) Treaty on the Functioning of the European Union.

2. Assessment of the proposed Art. 38 GDPR

With regard to the European Single Market, taking into account that drafting a code of conduct might be expensive and time consuming, entities will most likely not only address one single Member State. European-wide codes of conduct might be the preferred business approach. However, this would lead to a strange result. Supervisory authorities of a Member State, who would be responsible for enforcing the GDPR within this Member State, would only have certain rights with regard to the process of implementing a code of conduct. There would be no obligation to consult with such an authority before a code of conduct is adopted. Moreover, based on the current GDPR proposal, there would be no obligation to consult with the *European Data Protection Board*. The *European Commission* might only have second-hand information with regard to the implementation of the proposed GDPR. Therefore, there might be a risk for adopting a code of conduct, which is "problematic" from the point of view of supervisory authorities. It is an open question if a code of conduct can only be legally binding via an act of general validity. Furthermore, the practical benefit of such an act is vague. There are no concrete incentives for an entity to draft a code of conduct.

3. Proposal for modifications

As a result of a workshop by the *German Ministry of the Interior* in August and October 2012, a proposal for modifications with regard to Art. 38 GDPR was drafted.[71] The goal is to obtain a higher acceptance rate for self-regulation and to address the needs of practitioners.

The proposal limits self-regulation to the private sector. However, more entities would be allowed to use self-regulation. In addition to the proposal by the *European Commission*, there are references to Art. 6 (1) (f), 7, 23 and 30 GDPR. This should indicate, among others, the weighing of interests and technical measure for data protection. With regard to the administrative process associated with

drafting a code of conduct, it is proposed to publish each draft of a code of conduct as well as the intended change to an adopted code of conduct. Stakeholders should have the chance to state their opinions. The results shall be presented to the *European Data Protection Board.* This board can state its opinion and/or recommend the implementation of such a code of conduct. The general validity of a code of conduct should (still) only be a result of a decision by the *European Commission*.

This proposal is addressing the most important aspects of the drafting process with regard to a code of conduct. Criteria are stated in order to know aspects beforehand with regard to the weighing of interests, conditions for consents and with regard to the technical framework, especially with regard to data protection measures. This might be particularly useful for codes of conduct dealing with video surveillance and advertisements. In Europe, there are different points of view with regard to Privacy Law questions dealing with video surveillance and advertisements. European-wide codes of conduct, addressing the implementation of data protection provisions in these areas might help to achieve one single approach answering these questions. It is reasonable to have some sort of framework for drafting a code of conduct because besides these sets of rules, the drafting procedure is informal. It is uncertain if a legal obligation can be obtained by the general validity, based (only) on a legally binding Union act by the *European Commission*.

As an alternative idea, it might be possible to set up an "opt-out" procedure. Entities could draft a code of conduct and they could present their draft to their relevant supervisory authority. After accepting this draft as being in accordance with the GDPR, this draft could be forwarded to every other supervisory authority responsible for enacting the GDPR. There could be a deadline for comments. If an authority does not state any objections, it agrees on this draft. However, if an authority does raise any objections, the code of conduct will not become legally binding within this authority's Member State. The entity responsible for this draft could then decide if it wants to challenge these objections. This idea would provide for a fast process in order to obtain legal certainty and an entity could decide from a business point of view in which Member State it wants to argue for a legal validation.

4. Criteria in order to achieve a successful self-regulation framework

Even though self-regulation in Europe is only limited to addressing the implementation of data protection provisions, it is useful and helpful in order to avoid legal uncertainty with regard to applying undefined law concepts. Furthermore, it can be a guideline for applying discretionary powers. This is very important for European Privacy Law. European supervisory authorities are independent. Agreeing on the implementation of data protection provisions can only be achieved directly by an agreement or indirectly via judicial rulings. Drafting a code of conduct is expensive and time consuming. Therefore, it is obvious that each entity will assess the advantages and disadvantages before starting this endeavor. As a result, if it is important for any legislator and if it is important for supervisory authorities – not just because of the obligation under Art. 38 (1) GDPR – to encourage such an endeavor, there must be a low-threshold with regard to the process and the advantages of following through with it must be visible. It is understood that complying with Privacy Laws might be a business advantage, if there is a level playing field. Therefore there might be a chance to adopt a code of conduct.[72] The following criteria should be considered when revising the self-regulation framework in Europe:

a) Transparent proceeding for drafting and adopting a code of conduct

There is no need for a detailed proceeding with regard to drafting and adopting a code of conduct. This would only hinder the creativity of the involved stakeholders. However, transparency is a key to a successful self-regulation framework. Implementing data protection provisions could affect the person responsible for this data processing, a supervisory authority and each individual data subject.

Therefore, the necessary proceedings should be as transparent as possible. Every stakeholder should be able to obtain information from one single source, i.e. a central office. For example, every draft version of a code of conduct could be published on the *European Data Protection Board*'s website. This website could be used to inform stakeholders with regard to deadlines and consultation proceedings. In this way, acceptance and understanding of Privacy Law could be improved.[73]

b) More entities should be allowed to use code of conducts

It should be considered to allow more entities to use codes of conduct. Besides associations and qualified entities, groups of data subjects should be entitled to use codes of conduct, too. Even if this might create a form of "self-regulation at the expense of a third-party", the involvement of a supervisory authority should be enough to secure compliance with Privacy Laws.

c) Coordination of self-regulation

In order to avoid adopting codes of conduct contradicting each other, there should be a single central office, for example with the *European Data Protection Board* (Transparency of self-regulation). This institution could secure a certain level of quality by advising stakeholders before adopting a code of conduct. Furthermore, every ongoing proceeding and every adopted code of conduct could be published and made available for everyone.

d) Establishing an organization of voluntary self-regulation

There is no doubt that supervisory authorities are staying in charge, enforcing Privacy Laws, after a code of conduct has been adopted. However, as long as an entity is acting in accordance with a current code of conduct, it should trust the fact that a supervisory authority will not act against this entity. It would be a benefit, if there would be a private organization controlling the compliance of different entities with regard to codes of conduct. On the one hand, supervisory authorities could focus on other tasks. On the other hand, each sector could focus on its own needs.[74] A supervisory authority would only be asked to act if it is absolutely necessary.[75] In Germany, this has been proven as a good approach with regard to the protection of minors in Broadcasting and in Telemedia.

e) Incentives for self-regulation

It would be desirable, if there would be incentives and encouragement instead of demands and restrictions.[76] However, it is not possible to set aside Privacy Laws or to stop the enforcement of a supervisory authority. Therefore, the main incentive is the legal clarification within the European Single Market. After adopting the GDPR, Member States will only have limited powers with regard to enacting Privacy Laws (see Art. 81 and 82 GDPR). This is one of the main aspects of this single European approach. Therefore, the implementation of data protection provisions within a Member State will become very important and new questions will be raised. Some of these questions could be answered by codes of conducts and this would create legal certainty.

VI. Summary

In conclusion, there is self-regulation with regard to Privacy Law in the US as well as in Europe. However, because of the different general frameworks, these instruments are used in different manners. In the US, there is not one comprehensive legislative approach to Privacy Law. The understanding of Privacy Law in the US is different compared to the European understanding. Therefore, the US approach could be summarized as "authorization of data processing, if there is no reservation". Moreover, self-regulation can be used as an "substitute" for state or federal legislation. With regard to *FTC* enforcement activities, self-regulation is playing a vital role.

In Europe/Germany, self-regulation can only address the implementation of data protection provisions. Under no circumstance could self-regulation be used instead of legislation. Therefore, compared to the US, there is a narrow scope with regard to self-regulation. However, if the current proposed GDPR is adopted, as proposed by the *European Commission*, there is a great need for substantiations on the implementation of data protection provisions. This could be achieved by the instrument of self-regulation. Furthermore, someone needs to take into account that because of the heavy involvement of US companies in Europe, the GDPR might have a positive influence on the US take on Privacy Laws. This might be a positive side effect of our understanding of Privacy as a fundamental right.

Regulated self-regulation creates legal certainty. Undefined legal terms and discretionary powers can be addressed in a practical manner. This helps to apply Privacy Laws on a daily basis before the beginning of data processing. Therefore, acceptance and trust can be established. Furthermore, the drafting of a self-regulation concept has an allocative function within an entity (comparable with drafting Binding Corporate Rules[77]). To this extent, every successful implementation of a code of conduct might help strengthen the current level of data-protection.

From a German point of view, the main instrument with regard to self-control is not found in § 38 a BDSG but in §§ 4 (f) and 4 (g) BDSG. These norms are addressing data protection officials within certain entities. These data protection officials are helping to very successfully secure Privacy Law compliance. In order to hold on to this most effective tool of self-regulation, every effort should be taken on every level. This would prevent losing this tool, in general, after the adoption of the GDPR. If the currently proposed GDPR is adopted, only certain areas of application will remain for data protection officials in Germany.

About the authors:

Thomas Kranig

is the president of the Bavarian Supervisory Authority on Data Protection with regard to the private sector. Furthermore, he is a member of the advisory council of the Journal of Data Protection Law.

Stefan Peintinger, LL.M. (Georgetown),

is a legal clerk ("Referendar") with the district court of Munich and a doctoral candidate with Professor *Stefan J. Geibel*, Maître en droit (Université Aix-Marseille III), at the Institute of German and European Corporate and Commercial Law at the University of Heidelberg. His thesis is dealing with "price transparency with regard to German and European Civil Law".

The authors are thankful to Professor *Julie E. Cohen*, Georgetown University Law Center, for her advice and for her suggestions.

---

[*] This translation is for informational purposes only. Citations are translated, however, titles have not been translated and endnotes have not been changed in accordance with the Uniform System of Citation by the Bluebook. In general, citations are in accordance with the Beck Publishing Company's guidelines.

[*] This translation is for informational purposes only. Citations are translated, however, titles have not been translated and endnotes have not been changed in accordance with the Uniform System of Citation by the Bluebook. In general, citations are in accordance with the Beck Publishing Company's guidelines.

[1] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[2] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Annex to the Recommendation of the Council of 23rd September 1980, Nr. 19 lit. b): http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation; See *Tinnefeld/Buchner/Petri*, Einführung in das Datenschutzrecht, 5th edition, 2012, p. 71.
[3] Official Journal L 281 , 23/11/1995, p. 0031 – 0050.
[4] See *Tinnefeld/Buchner/Petri*, *supra* note 2, p. 58.
[5] *Petri*, in: Simitis, Bundesdatenschutzgesetz, 7th edition, 2011, § 38 a BDSG marginal no. 1; *Talidou*, Regulierte Selbstregulierung im Bereich des Datenschutzes, Frankfurt am Main, 2005, p. 27 ff.
[6] *Schröder*, ZD 2012, 418, 421; See *Finger*, ZD 2011, 109, 111.
[7] *Hornung*, ZD 2011, 51, 55; *Roßnagel/Richter/Nebel*, ZD 2013, 103, 106.
[8] *Gola/Klug*, Grundzüge des Datenschutzrechts, 1st edition, 2003, p. 110.
[9] See *Gola/Klug*, *supra* note 8, p. 111; *Abel*, RDV 2003, 11, 12.
[10] See http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/OH_Selbstregulierung.pdf.
[11] See *Petri*, *supra* note 5, § 38a BDSG marginal no. 21 und 27.
[12] *Karstedt-Meierrieks*, DuD 2001, 287, 289.
[13] Critizing current form of remedies: *Spiecker gen. Döhmann*, K&R 2012, 717, 723.
[14] *Weichert*, RDV 2005, 1, 2 f.
[15] *Spindler*, Gutachten F zum 69. Deutschen Juristentag, 2012, p. F 18 f.
[16] The so called "*Düsseldorfer Kreis*" is the association of all German State supervisory authorities on Data Protection Law.
[17] http://www.gdv.de/wp-content/uploads/2013/03/GDV_Code-of-Conduct_Datenschutz_2012.pdf.
[18] http://www.geodatendienstekodex.de/images/pdf/Datenschutz-Kodex.pdf?layoutId=54130; see ZD-Aktuell 2012, 03244.
[19] To the extent evident, this codex is only published as a "draft version": http://www.fsm.de/ueber-uns/veroeffentlichungen/FSM_Closing_Report_SocialCommunities.pdf.
[20] http://www.ddv.de/index.php?id=107.
[21] https://www.adm-ev.de/.
[22] A Robinson list is an opt-out list of people who do not wish to receive marketing information; http://ddv.de/index.php?id=380&L=0.
[23] *Gola/Schomerus*, in: Kommentar zum Bundesdatenschutzgesetz, 11. Edition 2012, § 38 a BDSG marginal no. 9; see Stellungnahme 3/2003 der Artikel 29-Datenschutzgruppe zum europäischen Verhaltenskodex von FEDMA zur Verwendung personenbezogener Daten im Direktmarketing vom 13.06.2003, WP 77.
[24] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp77-annex_en.pdf.
[25] See *Abel*, RDV 2003, 11.
[26] *Gola/Schomerus*, *supra* note 23, § 38 a BDSG marginal no. 6; *Petri*, *supra* note 5, § 38a BDSG marginal no. 25.
[27] *Kahlert*, DuD 2003, 412, 416; *Gola/Schomerus*, *supra* note 23, § 38a BDSG marginal no. 6.
[28] See *Solove/Schwartz*, Information Privacy Law, New York, 2011, p. 2; See *Rubinstein*, A Journal of Law and Policy for the Information Society 2011, 356; *Tinnefeld/Buchner/Petri, supra* note 2, p. 234.
[29] siehe dazu: http://www.ftc.gov/opa/2013/07/coppa.shtm; *Larose/Siripurapu*, National Law Review 2013, abrufbar unter: http://www.natlawreview.com/article/guide-to-compliance-amended-children-s-online-privacy-protection-act-coppa-rule.
[30] As already mentioned by *Spies*, ZD 2011, 12.
[31] *Talidou*, *supra* note 5, p. 207.
[32] *Tinnefeld*, DuD 2002, 231, 232.
[33] See *Solove/Schwartz*, *supra* note 28, p. 834; see *Rubinstein*, *supra* note 28, 356; *Tinnefeld/Buchner/Petri, supra* note 2, p. 234.
[34] *Talidou*, *supra* note 5, p. 76 ff.
[35] See *Rubinstein*, *supra* note 28, 356, 357.
[36] For the old version of COPPA: 15 U.S.C. § 6503; for the current version: 16 Code of Federal Regulations (C.F.R.) § 312.11 „Safe Harbor Programs".
[37] See *Rubinstein*, *supra* note 28, 356 f.; see the report by *Robert Pitofsky*, former *FTC* chairman, 21st of July 1998, "Consumer Privacy on the World Wide Web": http://www.ftc.gov/os/1998/07/privac98.htm.
[38] See *Kang*, Stanford Law Review 1998, 1193, 1253; see *Schwartz*, Connecticut Law Review 2000, 815, 833.
[39] See *Rubinstein*, *supra* note 28, 356, 357; *Spies*, ZD 2011, 12, 14.
[40] See *Rubinstein*, *supra* note 28, 356, 357 as well as 363.
[41] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[42] See Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation, 2012, p. 29; *Polenz*, VuR 2012, 303 ff.

[43] See Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation, 2012, p. 29 f.
[44] See *Rubinstein*, *supra* note 28, 356, 359 as well as 394 ff.
[45] http://www.asrcreviews.org/category/caru/.
[46] Self-Regulatory Program for Children's Advertising, p. 5: http://www.caru.org/guidelines/guidelines.pdf.
[47] See *Rubinstein*, *supra* note 28, p. 356, 369.
[48] http://www.dmaconsumers.org/privacy.html.
[49] http://www.networkadvertising.org/code-enforcement.
[50] http://www.truste.com.
[51] http://www.bbb.org/.
[52] http://www.privacyalliance.org/.
[53] http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc2.htm.
[54] http://export.gov/safeharbor/eu/eg_main_018365.asp.
[55] *Talidou*, *supra* note 5, p. 166; see *Rubinstein*, *supra* note 28, 356, 390 ff.
[56] See *Talidou*, *supra* note 5, p. 163 ff.; see *Solove/Schwartz*, Privacy Law Fundamentals, Portsmouth, 2011, p. 174.
[57] See *Talidou*, *supra* note 5, p. 164 f.
[58] See *Talidou*, *supra* note 5, p. 166.
[59] See *Talidou*, *supra* note 5, p. 170.
[60] *Schröder*, ZD 2012, 418, 421.
[61] *Rubinstein*, *supra* note 28, 356.
[62] See *Solove/Schwartz*, *supra* note 28, p. 893 as well as 899.
[63] See *Solove/Schwartz*, *supra* note 28, p. 826 f.
[64] as an example, See the website by the State Attorney General of California: http://oag.ca.gov/privacy; Website of the "*National Association of Attorneys General*" (NAAG): http://www.naag.org/cybercrime.php; see *Spies*, ZD-Aktuell 2013, 03417 and ZD-Aktuell 2013, 03739.
[65] See *Collin*, JZ 2011, 282.
[66] See *Tinnefeld*, DuD 2002, 231, 232.
[67] See *Kranig*, ZD-Aktuell 2012, 02910.
[68] *Tinnefeld/Buchner/Petri*, *supra* note 2, p. 234.
[69] *Talidou*, *supra* note 5, p. 210.
[70] *Schröder*, ZD 2012, 418, 419.
[71] Part of the Council's documents, dated 13th of February 2013 by the *German Delegation to the Working Group "Information and Data Protection"* (DAPIX), Nr. 6413/13: http://register.consilium.europa.eu/servlet/driver?typ=Advanced&cmsid=639&fc=REGAISDE&srm=25&md=100&lang=DE&ff_DOCKEY=%22ST6413/13ORI%22&rc=1&nr=1&page=Detail (so far this document is only available in German).
[72] See *Weichert*, RDV 2005, 1, 3; see *Kinast/Schröder*, ZD 2012, 207, 210.
[73] See *Karstedt-Meierrieks*, DuD 2001, 287, 289.
[74] See § 19 Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and in Telemedia (Interstate Treaty on the protection of minors – JMStV); see *Schröder*, ZD 2012,418; for the relevance of such an organization, see: OVG Berlin, NJW 2003, 840, 841.
[75] See Art. 38 a DS-GVO-E of DAPIX, *supra* note 71.
[76] See *Roßnagel*, MMR 2005, 71, 75; *Kinast/Schröder*, ZD 2012, 207, 210.
[77] for Binding Corporate Rules, see: *Filip*, ZD 2013, 51.