Collection of examples for possible impacts of the EU data protection regulation

The 10 most important demands of the ITC sector, illustrated by examples:

1. Differentiated application of data protection law
2. Lawfulness of data processing
3. Consent
4. Rule for data transfers in groups of undertakings
5. Differentiated regulations for profiling
6. Competence of advisory bodies and coherence procedures
7. Controller Processor Relation
8. Self-regulation and certification
9. "Right to be forgotten"
10. Delegated legal acts / framework for sanctions / bureaucracy

1 Differentiated application of data protection law

The draft of the data protection regulation provides a very broad concept of personal data; the scope would comprise data of any kind, as long as they can be - in pure theory - brought in connection with a natural person. This means the guidelines of data protection law need to be considered even where a violation of the concerned person's privacy can be excluded. The scope of the data protection regulation threatens to go over board and to reach out to areas of life that are not connected to the actual protection purpose of the regulation. Basic rights of third parties like the freedom of opinion and information or the right to free economic activity might be unnecessarily obstructed and bureaucratic obstacles may be created that could pose major burdens in particular to small and medium enterprises.

The application of the data protection regulation has thus to be restricted to the actual possibility of creating a connection between data and an individual person, since only in such a case the privacy right of this person might be concerned. In this respect we should follow the predominant idea of "relative personal relation" in Germany. Therefore it is essential that the processing organ can connect the data to a natural person with normally available tools and without disproportionate effort.

This definition ensures that the person concerned is protected if there is a realistic chance to connect the data to the person. At the same time, the exchange of data, information and opinion as well as the possibility of economic activity remains guaranteed, if the privacy right of the person concerned shall not be touched due to a lack of reference to a specific person. This creates a general incentive to anonymise or pseudonymise data at an early stage to exclude such a reference to specific persons. Very often there is neither a need nor an interest in processing personal data. For this reason it should be

German Association
for Information Technology,
Telecommunications and
New Media

Albrechtstraße 10 A
10117 Berlin-Mitte
Germany
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Contact
Susanne Dehmel
Head of Department
Data Protection
Tel.: +49.30.27576-223
Fax: +49.30.27576-51-223
s.dehmel@bitkom.org

Nils Hullen, LL.M.
Head of Brussels Office
Rue de la Science 14
1040 Brussels, Belgium
Tel.: +32.2.609 53 21
Fax: +32.2.609 53 39
n.hullen@bitkom.org

President
Prof. Dieter Kempf

Management
Dr. Bernhard Rohleder

made clear that the data protection regulation does not apply if data are anonymised.

In terms of pseudonymised data the same should apply as long as it is clear that the processing organ clearly separates pseudonym and clear name and does not re-establish the connection between pseudonym and individual.

- **Retrieval of websites**
  If a website is retrieved (e.g. http://axel-voss-europa.de/) the computer retrieving it transfers its IP address to the web-server to let it "answer" and provide the information where the Internet page has to be "delivered". Already during this procedure, the IP address will be processed by the web server.

  IP addresses are usually assigned only on a temporary basis in connection with certain Internet connectivity. Only the Internet provider of the accessing computer can assign the address to the owner of an access (but not to the actual user of the Internet access). The Internet provider may disclose the name of the owner of an Internet access only in cases established by law, e.g. for criminal prosecution purposes. The data processing organ or the operator of a website is not able to make such an assignment or make a reference to a specific person.

  Based on the definition of personal data in the draft, the IP address would be such a personally identifiable piece of data. This should be, however, excluded if the processing organ cannot make the reference.

  Processing IP addresses is necessary, e.g. for the optimisation of user-friendliness of a website. If IP addresses as such are considered personally identifiable data, a (supposedly) affected person might request information from the processing organ - the operator or the website. For them, however, it would not be possible to track back which IP address the person concerned had used, since he does not have the possibility to make a connection between an IP address and the owner of an Internet access (not to mention the user of an Internet access in a concrete case). The Internet provider cannot give the desired information. Even if the person concerned could provide their IP address with their request for information, it would not be possible for the Internet provider to check if it is true without retrieving further personal data.

  Contents of third parties on a website
  If contents of third parties are quoted or referenced on a website (e.g. with embedded videos, blog entries, etc.) retrieved by a user, the user's IP address has to be transferred to the third party to ensure that his content can be sent to the user. In such a case as well, neither the operator of the website, nor the third party has the possibility to make a reference to the person of the user with the help of the IP address. If IP addresses in general were considered personal data, the website operator would need to get the user's consent for transferring the IP address to a third party. This will be, however, not possible on a regular basis, e.g. for viewing journalistic internet pages (e.g. http://www.europeanvoice.com/) or information portals due to lacking user friendliness or complex accessibility of the information offer.

The economic benefit of online advertising is, on the other hand, crucial for all Internet offers, among others, in the field of quality journalism which is available to users free of charge. If such a possibility of funding through advertising is prevented although the processing organ (website operators or third parties transferring advertising banners) cannot track back the actual person, innovative business models on the Internet would be obstructed in all conceivable spheres.

- **Contracts for remote maintenance**
  Contracts for remote maintenance for storage systems or similar IT services, include the access to system data like IP addresses or error messages of the systems containing e.g. information on faulty storage media. Personal data saved on such a medium will not be transferred in such a process. So, we are dealing with data that cannot be tracked back and assigned to a person without any further information provided by the customer. As according to the definition of personal data in the draf, it cannot be excluded that such data needs to be assessed as personal data, in negotiations between the customer and the service provider comprehensive data protection clauses might be are under negotiation. In some circumstances the international transfer of such "personal data" will have to be secured by methods of 'safe harbour'' and 'model clauses.' This will result in additional costs without any positive effect on the level of data protection. In some cases the customer will have to - due to unclear definitions of the personal reference - insist that data is processed in Germany or at least within the European Union, although the data occurring in the framework of remote maintenance of IT systems cannot be connected to a concrete individual by the IT service provider. Due to the international specialisation of service providers, high level customer service is at stake. By excluding the 'follow-the-sun' model, which enables an international, current maintenance of highly complex IT systems, there will be further additional costs for the customer.

- **Fighting corruption**
  In the context of fighting and preventing corruption through pseudonymising personal data it has been possible so far to do an alignment of bank details without connecting the account information to a specific person. Persons were identified only and exclusively in concrete cases of suspicion. This minimal intrusion into the employees privacy rights successfully prevented millions of Euros of damages and has always been considered permissible by German supervisory authorities. Based on today's very broad definition of personal identification, an effective fight against corruption in such a way would no longer be possible.

- **Smart metering and the networked home**
  Smart metering and networked homes are technological innovations that are, among others, essential for the successful move to alternative energy sources. Providers of such services - e.g. energy providers - have no reason to retrieve personally identifiable data to offer customised services. According to today's definition of personally identifiable data, even providers offering a simple service like the transfer of the time would process personally identifiable data since they are processing IP addresses (which do not give the possibility to track the person concerned, see above). The same is true for eco-

logically necessary smart meters that also transfer the measured data to the provider or intermediaries via IP addresses and IDs of measuring points.

- **Expansion of non-automatic data processing procedures**
  The expansion of the scope of application of the data protection regulation to non-automatic data processing procedures would entail that every piece of paper with a note about a person in an office (e.g. telephone notes) would need to be disclosed in the case of an information request.

2 Lawfulness of data processing

The necessary data processing procedures in a business environment must be simple to implement - i.e. based on balancing of interests (also in favour of third parties). Circumstances under which permission is currently granted are narrower and less flexibly defined than the ones we know based on a guideline or the Federal Data Protection Act in Germany. They prevent acknowledged and necessary economic processes and can also become an obstacle to data processing procedures that become necessary in the future.

- **Debt collection and credit agencies**
  A consumer makes an order with a mail order company that stores the data. If the consumer does not pay the order, the data can be transferred to a debt collector in order to enforce the claim. This is in accordance with the EU data protection regulation. But if the mail order company transfers the data to a credit agency to process more orders placed by the same consumer or with other mail order companies, then this change of purpose is no longer covered by the EU data protection regulation, because it no longer coincides with the original purpose (order with a mail order company and processing of the order).

- **Pre-contractual and non-contractual credit rating**
  In terms of credit rating it is quite common and essential to illustrate a person's or a company's credit rating with a number (a score) in order to give the recipient of information a first and easy overview of the credit rating. In order to keep such procedures possible, it is necessary to extend the limitation of permissible data collection in Article 20 par. 2 lit a) on the conclusion or the fulfilment of a contract. It has been disregarded in so far that clients of credit agencies commission credit ratings also beyond existing or future contractual relations. This also applies to cases when a lawyer or debt collector wants to check the success perspectives of insolvency proceedings with the help of credit rating. A contractual relationship to a debtor does not exist in such a sense that the EU regulation could prevent to perform credit rating.

- **Sale against invoice in online sales**
  Without credit ratings sales against invoice would not be an option e.g. for online mail order companies because the risk of loss would be too high. Risks cannot be added to the price, because then, these companies would no longer be able to offer competitive prices (and that would not be in the customer's interest). Many customers prefer to order against invoice - in particular if they buy at mail order companies they are not yet familiar with; most customers may use this payment method. If there were no longer possibilities of uncomplicated credit rating before entering a contract, this would be incon-

venient for customers and would lead to significant downturns in turnover for the companies.

- **Advertising networks and website analytics**
  Right now the draft contains no provision comparable to § 15 par. 3 German Telemedia Act. This paragraph allows the use of pseudonymised user profiles for the purpose of advertising, market research or custom design of telemedia. The service provider is called upon to use technical and organisational measures to ensure that the user profiles cannot be connected with the information leading to the identification of the pseudonym's user (§ 13 par. 4 lit. 6 Telemedia Act). Without such a legal basis, service providers would no longer be able to analyse the contents of their website (e.g. to find out how popular a certain area is or if the navigation is user friendly). Moreover, it would no longer be possible to provide target group specific advertising. § 15 par. 3 Telemedia Act, on the other hand, harmonises the interest of the people to prevent personal user profiles and the industry's interest to evaluate the users' behaviour for statistical data.

- **Data processing in the interest of third parties**
  Right now there is no provision whatsoever to provide a permission in accordance with § 28 par. 2 lit. 2a German Federal Data Protection Act for data processing that is required to safeguard the legitimate interests of third parties. Many data processing procedures carried out by debt collectors or credit agencies are performed in the interest of their customers. If this possibility ceases to exist this would entail significant consequences for established business models and the companies making use of their services. Other examples show as well that such exceptional circumstances remain important, e.g. for the transfer of data to defend rights, as far as no other legitimate interests of the persons concerned prevail.

  Pre-contractual and non-contractual credit ratings (see above) would not be possible if the corresponding credit agencies and warning systems do not have the data base to develop corresponding scoring systems. Credit agencies and industry warning systems that are partly already legally required to prevent money laundering or fraud (cf. § 25 c German Banking Act) retrieve their data, as commonly conceived, not based on the interest of the bodies providing the data or the credit agency storing the data or the warning system, but based on the legitimate interest of third parties in the systems. If the legal basis protecting the interests of third parties ceases to exist, credit agencies and warning systems would not be able to become active at all since the transfer of corresponding data (in the interest of third parties) would no longer be permitted. In this respect, companies would lose the possibility to check credit ratings or use systems in the framework of compliance measures (for the significance of credit agencies, also check European Court of Justice of 23 Nov. 2006 – case 238/05).

- **Company Agreements**
  The regulation does not mention company agreements as permitted legal basis for data processing. It corresponds with the common German practice that certain data processing procedures, which are essential for a company, are aligned with the employees' interests by negotiating a company agreement with the works council. E.g. every company needs to rely on a function-

ing IT system which partly requires e.g. when security checks are performed - a check of employees' hardware or e-mail accounts. A company agreement can help to regulate the employer's access in a transparent and fair manner.

3 Consent

The number of cases where consent is needed instead of a legal permission is already high enough and shouldn't be extended as this might produce an obstacle to transparency. Data subjects have to face a number of single agreements and/or lengthy declarations of consent which are usually not read through thoroughly by the people concerned. At the same time, obtaining consent should not be overformalised, but consider the technical surrounding. Sufficient transparency guaranteed it should also be possible to give implicit consent. Companies efforts to make their processes as "minimally invasive" as possible should get rewarded by leaner requirements for obtaining consent.

Flexible measurements

Therefore measures should be flexible and consider the actual risks of the persons involved. E.g. for the Federal Court of Justice in its ruling on the "Payback" bonus programme permitted in principle that data protection consent is provided as an opt out, while the consent for direct marketing measures requires an explicit consent (cf. Federal Court of Justice BGH of 16/07/2008 - VIII ZR 348/06). Another example for flexible measures can be found in § 15 par. 3 Telemedia Act which does not require any consent as long as the user has the possibility to opt out.

Implicit Agreement

- An example for implicit consent is the "do-not-track" procedure. Consent is given implicitly by way of browser settings. The user declares their wish that their surfing behaviour must not be tracked with cookies or any other technical gadgets, or that the use of such technical tools is desired.

- Another possibility for an implicit consent is the receipt of information of a navigation system on the current traffic situation. The navigation system usually does not provide a possibility to agree explicitly in the transfer of location data that make it easily possible for the recipient to track back to the user's identity.

- The possibility of declaring consent has to be retained for legitimate data processing, since this is the only way to react flexibly to special situations that are not regulated by the current legislation. Moreover it is possible that an entrepreneur wants to get a consent if the legal situation is unclear, e.g. if a law is not clearly formulated, to be on the safe side in terms of data protection. Therefore it is not correct if (as it is suggested) to exclude a consent in an employer-/employee- relationship completely.

Burden of proof

The rule on the burden of proof in Art.7 (1) creates an unnecessary disadvantage for controllers and will force them to collect and archive more data in order to be able to proof given consent. Therefore it should be deleted. Already now usually companies have to proof that consent was given, if that is the legal basis for their processing – they have to provide processes for the declaration of consent and its filing. If they can proof that there is a filed consent, the burden of proof should go to the data subject that might still deny any declaration of consent. But then the data subject has to provide evidence why there was still no valid consent. The possibilties of anonymized usage of internet services shouldn't lead to a one-sided disadvantage for the Controller. Furthermore the relationship between Art.7 (1) and Art.10 is unclear as Art.10 says that the controller doesn't have to collect additional data merely for the purpose of complying with provisions of the regulation. But to comply with Art.7 (1) this would be necessary.

Significant imbalance

According to Article 7 par. 4, the agreement does not serve as a legal basis for the processing of data if there is a substantial imbalance between the position of the person concerned and the person in charge of processing the data. Such an imbalance has to be assumed very often if consent for data protection needs to be obtained in connection with signing a contract, especially if this applies to consumer contracts. However, in such cases it is very often essential to obtain consent and/or process data.

- For instance, it makes absolute economic sense that customers agree to obtain a SCHUFA ("Schutzgemeinschaft für allgemeine Kreditsicherung e. V." – German General Credit Protection Agency) report in order to conclude a current account agreement. If you want to enter a mobile phone contract, it is also a prerequisite to give consent to credit rating. If providers cannot obtain information on the risks of payment defaults they have to counter the risk by other measures (by increasing their prices). At the same time, when you conclude a health insurance contract, it is often necessary to give consent a release from the pledge of secrecy.

- The consequences of Article 7 par. 4 can have a sustainable impact on the person concerned. Once a managing employee signs a working contract in a company, he might no longer give consent to have his data in the company's internal talent data base and to be considered in corresponding promotion programmes.

- Many internal regulations on data protection are based on company agreements or consent - without them many voluntary actions of employers, e.g. share holder programmes, would not be possible. Moreover, using an e-mail account or an Internet access for private purposes might be prohibited by the company. Employees, on the other hand, expect to do this in many companies. A prerequisite for this is that the employee agrees that the company may recognise and filter faulty files or has access to business correspondence, e.g. when an employee is sick. Without this consent the company runs

the risk of violating the secrecy of telecommunication, which might become criminally relevant.

4 Rules for data transfers in groups of undertakings

In terms of the transfer of personal data into third countries or international organisations, the current draft of the regulation comprises many points to make cross border use and processing of data more flexible while creating more legal security for companies active at an international level. However, there is still no clear provision on data transfers between companies of a group which pays due attention to the interaction in labour division and the single economic unity of holdings. Organisational structures in holdings go more and more beyond companies and are oriented at product groups or project activities. The flexibilisation envisaged also presumes the availability of personal data for more than one company. Within a holding and especially for companies working at an international level, regulations regarding data protection are very limited for the transfer of data e.g. employee data within a group; the same clauses apply here as for the transfer of employee data to external third parties. This has an impact on numerous constellations.

- **Employee data**
  Within the matrix structure, employees are reporting to superiors who are not employed in the same company. The integration of superiors in personnel measures requires the access to personal data of employees reporting to them. Moreover it is necessary to create common systems for vacancy notices and applications, for the joint use of IT systems, for interorganisational management and talent development, for searching best candidates when filling vacancies (internal planning of careers and successors), sending personnel to international projects and assembly works and many others.
  The internal planning of succession can be driven purposefully only if the whole holding searches for talents and manages them. Otherwise only candidates from the relevant legally independent company unit could be considered.

  Internal training is only feasible efficiently if the corresponding training is offered for several companies within the holding (only if it is allowed to address everybody in all company units this will happen, otherwise the high effort of obtaining consent will lock out smaller legal entities/companies in particular).

- **Customer data**
  If it is not permitted to use a common CRM system, a holding cannot address their customers with one voice or manage them adequately. The customer is not aware of the structure of a holding in single units - he assumes anyway that everything belongs together under the same "brand".

- **Economic server structures**
  Single-sign-on models for two companies within a holding should be possible. There will be an increasing number of cases in which several systems have to communicate to create more service and comfort for the user, and to work more efficiently for the company. Moreover, only unified intelligent server structures make significant energy savings possible at a worldwide level.

5 Differentiated regulations for profiling

Changing the formulation of Article 15 of the Data Protection Directive 95/46 in the regulation draft requires clarification which of the profile structures permitted so far shall remain active. From a company point of view it should be possible to create profiles if there is a legitimate interest of the controller and there is no prevailing interest of the data subject and/or there is no fear of a harmful decision for him.

- Giving privilege to anonymised or pseudonymised data enables the processing organ to create user profiles, e.g. for advertising, market research or for adequate design of Internet services, without violating the rights of the people concerned. This corresponds with the legal situation in Germany (cf. § 15 par. 3 Telemedia Act) which enables a balance satisfactory for all interests. This privacy-enhancing creation of profiles is clearly different from profiles that connect user activities to an individual and can therefore legally take place also without the explicit consent of the person involved.

- Creating profiles in the context of credit scoring is a necessary instrument of balancing risks to legitimately exclude certain payment methods offered in e-commerce and prevent significant payment defaults (e.g. blocking orders upon invoice after delivery of an item with pending payment of the same user).

6 Competence of advisory bodies and coherence procedures

The introduction of a one-stop-shop-principle for all competences of regulatory bodies (Article 51) is welcomed as well as the principle of coherence procedures for regulatory bodies. The current design of regulations does not seem to be appropriate to achieve neither the goal of a real one-stop-shop nor continuous law enforcement.

- If a group of companies (e.g. a holding) consists of several legally independent entities, e.g. two GmbH's, an S.A. in France, a Ltd. in UK and an SpA in Italy, there are five controllers and we still have four to five competent supervisory bodies. It would be necessary to have a regulation in which companies, who are shareholders of each other or dependent on each other in accordance with § 18 Stock Corporation Act, are within the competence of the supervisory body of the supreme company, alternatively the largest (by turnover, number of employees, scope of IT) in the European Union.

- A German company operates a delegation centre in the Czech Republic. It coordinates international placements of employees within the holding. This is a relatively complex task due to visa regulations, social security regulations, pension funds, relocation support like apartment search, school search etc. Therefore these services will be bundled and performed by the Czech daughter company. There is a supervisory body in charge of the German company and one for the daughter company. One of the advisory bodies assesses the data transfer to the daughter company as data transfer, the other as data processing on behald. Therefore this process could not be assessed uniformly. Such constellations usually cause preventable bureaucratic processes and legal uncertainty. In such cases it is even possible that decisions taken by two supervisory bodies are absolutely contradictory: one says that a process is

possible; the other one says it is not. In such a case, a company is in a catch-22 situation.

- Referring to the "main establishment" does not necessarily work in practice, as e.g. the following case shows: the headquarters of a company are located in Luxembourg, but all other national data protection organs cannot accept this and still address the other offices if they take their own decisions. Therefore it might be helpful to use the criteria defined by the Commission itself for BCR's to define the lead authority (also cf. http://ec.europa.eu/justice/policies/privacy/binding_rules/designation_authority_en.htm).

7 Controller and Processor Relation

Clear regulations for data processing on behalf - in particular on dividing the competencies and responsibilities - are essential to the further development of cloud computing and the value added for the whole European economy. It depends of the practicality of these instructions if such new business models are rather promoted or obstructed. The regulations proposed for data processing on behalf do structurally not fit to some forms of cloud computing and make them more complex. In order to become practical, the regulations proposed need to be thoroughly reviewed to clarify that the figure of data processing on behalf is a legal permission for transferring data for a specific purpose and in the framework of a specific contract. The controller must be able to refer to objective criteria that help him to assess which processor he can trust.

- **Infrastructure provider**
  The processor who is according to the draft responsible for the data he processes like a controller, very often does not have the possibility to take notice of the content of the data, e.g. if he only transports them in an encrypted form, stores or archives them. An infrastructure provider in the case of cloud computing will have no access to the data processed in his container. Making him responsible for the data of his customers forces him to look into the data and is as such not beneficial for data protection. The benefit of encryption is contradicted. A differentiation of actors would be appropriate. Processors that do not have the possibility to learn about the contents of data should be excluded from the scope of the regulation. For example, if premises are rented for the use of infrastructure, this does not increase any risks, because the data are not accessible. A clear definition is necessary to define where "handling data" starts.

- **Remote maintenance of systems**
  Providers who don't have an interest in the data, but need to access them from time to time, e.g. for remote maintenance, should be exempted from documentation duties. A corresponding regulation like § 100 German Telecommunications Act could be integrated. It states that the service provider does not act as processor: "As far as necessary, the service provider may generate and use the inventory data and traffic data of participants and users to identify, isolate and remove errors."

- **Sharing duties and powers**

Moreover, processors should be responsible only for the duties within their tasks, e.g. taking necessary protective measures (e.g. privacy by design) and use appropriate security systems. In that sense, customers who are certified as corresponding to security standards in advance may rely on this without fulfilling any additional control duties on their own behalf.

- **Joint Responsibility**
  There are no examples for a joint responsibility for processing, in which a concentrated responsibility of the controller was not preferential for the parties involved, from the perspective of the person concerned as well as for internal coordination between the controller and the processor in e.g. the performance of the "right to be forgotten" as well as the duties on information and documentation. Duplicating these tasks in the framework of a joint controllership (Article 24) increases the efforts of alignment and documentation duties inadequately. This would mean that both have to document identical situations, to hand in a privacy and data protection impact assessment and provide information to requests without providing an improvement from the perspective of the person concerned compared to the current legal situation. Regulations on the common responsibilities are also difficult with regard to information obligations towards data subjects and in terms of the supervisory bodies. The bureaucratic efforts do not lead to an increase of data protection and mean an obstacle to innovation.

- **Disadvantage for European Processors**
  The regulation in Article 3 par. 1 poses a disadvantage to contract data processors based in Europe who provide their international services from this location: they have to comply with the regulation even if their clients (and/or their personally identifiable data have no other reference to Europe. This increases administration and costs and might even lead to international uncompetitiveness, e.g. for helpdesk applications.

8 Self-regulation and certification

This regulation is supposed to anchor the topics of self-commitment and certification and create a practical framework for it.

- **Codes of Conduct**
  Numerous approaches for self regulation (binding corporate rules, accountability, data protection officer, codes of conduct...) do already exist. However, there is no systematic development of the instrument of codices. The current European data protection law provides already a basis for codes of conduct as legal instrument in Article 27 of the Data Protection Directive; however, their approval by data protection authorities has been regulated only insufficiently and has only happened in very few cases.

  In Germany we have so far not a single completed procedure in accordance with § 38a Federal Data Protection act that implements Article 27, so there is no officially recognised behavioural codex. If we analyse previous projects, this might be partly the case because the necessary informal alignment processes of the supervisory bodies take their time and at the same time it is unclear if the recognition of one supervisory body is binding for the others and if the codex as such needs to go beyond the level of legal regulations or

if it is sufficient to comply with the legal regulations and/or make them more concrete.

In order to avoid insecurities we have had so far, this regulation should provide explicit rules for the following topics:

- Self-regulation is supposed to concretise the legal framework without necessarily going beyond that. The regulation should give associations or professional federations a right to get a code of conduct approved by the competent supervisory body in adequate time, if it complies with the provisions of the regulation.

- If the approval is denied or if the supervisory body in charge does not become active, legal procedures for the clarification of controversial legal questions are required. At the same time, the legal means for judicial review of the decision need to be installed.

After the experience with previous codex projects from the companies' perspectives the following conditions for the participation in codes of conducts should be given:

- **Legal certainty:** More legal certainty and/or reduced risk of sanctions imposed by supervisory bodies by joining a code of conduct. This needs a stringent interpretation of the law by the different supervisory authorities as well as mechanisms for conflict resolution for the clarification of controversial legal issues that do not make specific companies a public example.
- **Reduction of complexity:** Acceptance of (possibly certified) self-regulation by supervisory bodies and customers as proof of correct implementation of necessary data protection measures (in accordance with § 11 II 4 Federal Data Protection Act).
- **Cost control:** Costs for self-regulation have to be in proportion to the benefits gained by the companies by joining the cause of self-regulation.
- **No special option for single nations:** Self-regulation should be recognised within Europe and - ideally - internationally. It is not supposed to come on top of the legal provisions, but to make them more concrete.
- **Right to approval**: Companies should get a right to obtain the approval of a code of conduct if it corresponds to the legal requirements.

- **Certification**

An important application is contract data processing. Persons responsible for the processing of personally identifiable data are obliged to select the service provider with due diligence in terms of data protection and carry out controls thereof. For providers of comprehensive services (e.g. in cloud computing) it is of special importance to certify them. This is the only way to prevent numerous single controls by the clients or in the framework of selection decisions.

Certification possibilities are supposed to follow unified, objective standards that make it possible to compare providers and their data protection measures. Therefore it is necessary to create options that take into account the degree to which data need to be protected. E.g. medical data or data un-

der professional confidentiality must be secured with a higher standard than the address data of an online lottery.

Providers should be able to commit themselves by established standards to an appropriate package of measures and then get certified. The procedure has to be designed in such a way that supervisory bodies can rely on it.

9 "Right to be forgotten"

The draft regulation gives every person the right to demand "to be forgotten". The objective of this right is to give the data subject - in particular in view of the internet - the possibility to cancel the availability of or the possibility to use their data again. From the industry perspective, this approach is absolutely understandable, but the current version of Article 17 of the draft regulation does not contribute to more effective data protection.

- The requirements of the data processing body remain to be clarified in concrete cases. Constellations are problematic where a user first registers with a social network and enters information about himself and others that he wants to delete selectively at a later point and realises that his photos are present on other pages as well. All concrete duties of a network provider are under question if a user wants to leave a platform on the whole and/or wants to switch to an alternative provider. This existing legal uncertainty questions business models on the Internet that are used and appreciated by millions of EU citizens on a daily basis. But not only social networks affected, but also controllers of all kinds, as the “right to be forgotten” is not limited to certain constellations.

- In order to ensure that all copies of information once published within a service can be deleted, the person concerned has to track their contents - which is not desirable from a data protection perspective.

- Problems do also exist in the relation between the rights of data subjects and the freedom of opinion of third parties: discussions in Internet forums or other platforms might become absolutely worthless once single messages in a thread get deleted. It is difficult to draw the line between freedom of opinion and data protection. Therefore it needs to be safeguarded that everyone can decide for themselves if they want to participate in a public discussion. If they do that, it is under question if they can readily distance themselves and/or may delete all contents. Also in the "offline" world we cannot demand newspaper publishers who wish to produce coverage of facts in the public interest to delete singular quotes which are interesting for the general public. The same must be true for the freedom of opinion and information for the world "online".

- There are the following difficulties from a technical point of view: A duty to delete exists also for cases in which the person concerned is no longer controlling the data. These provisions cannot be fulfilled in practice.

10 Delegated legal acts / framework for sanctions / bureaucracy

The big number of delegated legal acts as provided in the regulation draft leads to significant legal uncertainty and should be reduced.
In addition, stricter sanctions need to be examined against the background that the majority of companies require data processing as a necessary tool to do business and that only few make data collection and processing a business as such. Therefore sanctions that threaten the existence of companies are out of proportion to the severity of negligent violations. Moreover many provisions are too uncertain to connect them to harsh sanctions. There is a continuing disproportion to sanctions in the public sphere. Moreover the draft regulations contain too many documentation duties and unnecessarily complex procedures that incur high costs without improving the level of data protection.

- **Penalties**

  The draft regulation contains numerous disproportions between violated duties and possible sanctions.

  - According to Article 79 par. 6 a everyone has to face a penalty of up to 1,000,000 Euro or in the case of a company up to 2% of its worldwide sales per annum in case of a negligent violation of the terms of consent when processing personally identifiable data. This is totally in disproportion to the framework of sanctions with other, significantly more serious, violations in the business world. For example, if someone in Germany deliberately builds a dumping ground without planning approval decision or planning permission, has to face a fine of 50,000 EUR maximum according to the German Recycling and Waste Management Act.

  - Moreover, many duties arising from the data protection regulation for the processing organ are not concrete enough. Against this background, the harsh possible sanctions are especially problematic due to the principle of certainty. We would like to cite Article 23 as an example in with the requirements for data protection through technology and privacy by default are not sufficiently clear. Still, negligent omission or wrong usage can already lead to harsh sanctions (Article 79, par. 6, lit. p): penalties of up to 1,000,000 Euro or in the case of a company up to 2% of its worldwide sales per annum.

  - Connecting a penalty to the sales is also problematic because there are dramatic differences between the profit margins of trading companies and service providers. Companies with a higher turnover do not necessarily make profit. Start ups in particular and new business models can be ruined by high penalties that are linked to sales figures. In addition, it is not plausible why the turnover should serve as an assessment basis for penalties in the case of violation of single persons.

- **Documentation duties**

  The draft regulation contains a list of unnecessary and complex documentation duties. E.g. Article 26 par. 3 of the draft provides that the person in charge of processing as well as the contract data processor shall document the instructions of the commissioner and the duties of the contract data processor. At the same time, Article 28 provides for a number of double docu-

mentation duties of the people in charge and the contract data processor without obvious compelling reasons. This is also true for Article 22 par. 2 lit. a referencing Article 28.

- **Delegated legal acts / Implementing acts**
  The draft regulation provides a number of delegated legal acts and implementing acts with problematic consequences.

  - According to Article 6 par. 5 the Commission will be authorised to enact delegated legal acts to provide for the concrete regulation and the application of Article 6 par. 1 lit f for different areas and processing situations. Article 5 par. 1 lit. f provides for balancing of interests. Balancing of interests may, however, lead to the consequence that some critical decisions of the regulation can still be changed.

  - According to Article 18 par. 3, the Commission can define the electronic format for data processing and technical standards, modes and procedures for transferring data. Such a definition, however, has direct effects on the usage of certain procedures.

  - According to Article 79 par. 7, the Commission shall be authorised to enact delegated legal acts to update the amounts of penalties. This is also a very problematic regulation because some of these critical decisions should not be taken at the Commission's discretion alone.

  Finally, the implementation period of 2 years is contradicted if the Commission is authorised to enact new provisions any time.