HDE
Handelsverband
Deutschland

[Lobby register
No.: 31200871765-41]

Position Paper on the Proposal for a Regulation of the European Parliament and 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)

COM(2012) 11/4 from 25 January 2012

I. Introduction

Established over 90 years ago, the German Retail Federation (Handelsverband Deutschland – HDE) is the head organisation of the German retail sector for approximately 400,000 independent companies with a total of 2.8 million employees and a combined turnover of nearly 400 billion euros. The HDE supports the interests and needs of the whole retail sector - for all types, all locations and all sizes.

II. General Remarks

The HDE welcomes the aim of the proposed regulation to harmonise and modernise the European data protection legislation in order to address the challenges of the increasingly global and digital economy. Harmonised and appropriate data protection standards within the EU could raise the competitiveness of the European economy by cutting red tape, decreasing costs and increasing the legal certainty for companies and consumers. To achieve this however, over-regulation must be avoided and data protection standards will not be geared towards the highest level of existing national rules.

Within the retail sector the issue of data protection is of great significance. In the daily dealing with their customers, employees and suppliers, companies process – among others – personal information. As retail companies are confronted with data protection regulations in nearly all of their fields of activity, data protection should be regulated as practicably and unbureaucratically as possible.

1. Compatible regulation for all parties

The challenge lies in wording the generally applicable provisions in a way that is proportionate for the economy as a whole as well as consumers. In the past the approach of codifying generally applicable data protection regulations - which had to be adhered to under all circumstances - had proven to be very successful. In line with this experience setting rules which are primarily aimed at certain internet-based services (e.g. search engines or social networks) should by all means be avoided. From our point of view, effective European data protection legislation has to be based upon rules and principles which are generally applicable. It has to be applicable to a retail company - which has built up a customer database to support its core business – as well as social networks – whose core activity lies in processing user information for advertising purposes. In doing so, it is therefore also necessary to balance the economic interests of processing data, of low costs and a low administrative burden with the reasonable consumer interest of protecting personal data.

2. Reservation of authorisation sustainable?

Companies increasingly depend on the processing of personal data. This ranges from human resource management departments (e.g. salary management, employee health, social benefits such as company nurseries) or office communications to marketing and logistics. Against this background, it is generally questionable whether the general ban on processing personal data with reservation of authorisation is currently still productive and accommodates the large number of

practical applications and future technical developments. A systematic change should therefore be considered which would generally authorise the processing of personal data and would only be illegal in case of clearly defined offences. General clauses with the obligation for self-assessment should, however, be avoided as this would lead to unnecessary legal uncertainties and – due to risk prevention – a de facto disproportionate limitation of the freedom to operate.

Should the system of bans of reservation of authorisation be upheld, in our opinion at least a risk-based assessment of the data processing situation with regards to the interests of the data subjects and the legal protective measures in place should be undertaken.

In this regard the inclusion of the so-called listing privilege as authorisation – i.e. the possibility to use certain personal data (e.g. name, address, profession) for advertising purposes or for the purposes of market and opinion research even without consent and within certain parameters to pass on to third parties - would be desirable. The exception recognized under the German data protection law would offer a balanced model which provides sufficient protection for the person concerned. According to article 28, paragraph 3 of the Federal Data Protection Act (BDSG) the use of data is not allowed if it can be assumed that this would infringe the interests of the data subjects who are entitled to protection. This is especially the case when the person concerned has vetoed of the use of his data (opt-out). Furthermore, the advertising has to clearly identify the organisation which originally collected the data.

3. Flexibility in the regulation

Within the context of the existing data protection directive (95/46/EG), sector-specific regulations in self-contained guidelines were published corresponding to the framework of the principles of the data protection directive. In this manner, the technological development could be taken into consideration without having to regularly revise the actual data protection directive. According to the proposed regulation, in the future this flexibility should be ensured by delegated legal acts of the European Commission. By means of delegated legal acts the European Commission would therefore determine in future how the data protection rules should be applied to entire economic sectors.

These important adjustments should in no case be undertaken in a way that eliminates the proper legislative processes. From our point of view the flexibility of the data protection law has to be ensured without passing on such far-reaching competencies to the European Commission as outlined in the proposal. Therefore, regardless of the fast-moving technical developments, it should be ensured that as many material legal details as possible are described as precisely as possible in the regulation itself and that the delegation of competences is limited to technical details with no practical implications on the material regulation itself are impossible. Any other option would result in a limitation of freedom of operation and operational certainty for companies without adequate democratic legitimation and would endanger the acceptance of the whole European codification in an undesirable manner.

III. Detailed comments on the General Data Protection Regulation

1. Scope of application (articles 2, 3)

HDE welcomes that the regulation includes the data processing of companies established in as well as outside of the EU insofar as it concerns the data subjects living within the EU. Only in this manner, legal avoidance by moving headquarters and distortion of competition can be avoided. However the question for us is how adherence should be guaranteed in practice, e.g. in the case of companies which are established outside of the EU but who sell their products via the internet to customers in the Single Market.

Moreover, it is not comprehensible why according to article 2 paragraph 2b) the institutions, bodies, offices and agencies of the EU should be exempted from the material scope of the regulation. It is one of the core characteristics of a constitutional democracy that also the public institutions are bound to applicable laws and legislation. Should the EU Commission only wish to pass data protection regulations to which it cannot or will not guarantee adherence itself then this should be cause to test the practicability of the planned regulation and deregulate accordingly where required.

2. Definitions (article 4)

a) „Data subject“ / „personal data“ (paragraphs 1, 2)

The definition of “personal data” is too broadly defined in our opinion. This is caused by the definition of “data subject”. It is not possible for the controller to evaluate whether “any other natural or legal person” (e.g. a bank, the postal service, Google) has the means to identify a person directly or indirectly. However, according to the definition exactly this criterion defines whether data is “personal” or not. Consequently all data which *could* be used to identify a person – independent of the possibilities, which are disposable to the controller – in principle would have to be classified as personal data and protected accordingly.

This constellation would be a complete renunciation of the risk-based approach. This rule would complicate all economic activities which include data processing and cause unnecessary red tape without improving the protection of the privacy of data subjects. Hence, the definition should be limited to persons who can be identified by the controller with the means reasonably likely to be used.

The terms “physical, physiological, genetic, mental, economic, cultural or social identity” are not explained in any detail and hence cause further legal uncertainty. As the list is not conclusive and indicative, it should be considered to move this part of the definition into the recitals. Considerable legal uncertainty is also caused by the undefined legal terms “means reasonably likely”. Here a precise explanation is needed.

Crucial limiting factors for the assessment of the existence of personal data are presented in recital (23). We believe a differentiation between data of “identified or identifiable” persons and data rendered anonymous would be sensible. However, an additional explanation of the limits of anonymisation would be helpful here. The limitation in recital (23) – that the principles of data protection should not apply to

anonymised data – should be explicitly stated within the regulation text. An inclusion of a definition of “anonymised data” in article 4 would be a possible solution.

b) „Data subject’s consent” (paragraph 8)

The definition of consent is especially problematic regarding the “explicit” statement of intent as it would result in companies having to obtain several separate consents for every specific data processing and this would cause substantial bureaucratic efforts and costs.

For transparency reasons the option of an “opt-in” was chosen. The question is whether in this context also an “opt-put” would be sufficient or whether a standardised consent via the general terms and conditions would be possible. In either case practicability has to be ensured.

The next question is whether an implied consent would not be sufficient. In our opinion recital (25) should be understood to that effect. This should absolutely be clarified in the definition of “consent” itself in article 4.

3. Lawfulness of processing (article 6)

a) Limitation to purpose (article 6, paragraph 4)

The strict limitation to the purpose of the data collection as basic requirement for the use of data in article 5 b) and article 6 paragraph 4 is problematic insofar as it would prevent the use of data - which were lawfully obtained through a contract – for any other purpose, for example address trading, credit worthiness checks or in-house banning notices as well as targeted advertising campaigns. This would have significant financial implications and also addressing new clients would no longer be possible. It is unfortunate in this context that, while exceptions to this rule are foreseen – e.g. through consent (paragraph 1 a) – nevertheless, the justifiable interests of the company which has collected the data, is not included here (article 6, paragraph 1 f) and therefore the scope and reasoning of article 6, paragraph 1 f) are limited in their effect. A differentiation with regards to the content of the data should be considered as the danger of misuse and the risk for the data subject will always depend on the content and extent of the data collected. Therefore, an exception regarding the strict limitation of purpose should be included following the example of article 28, paragraph 3 of the Federal Data Protection Act (BDSG) which exempts data collected in lists or summaries of data which are limited to information on profession, branch, business relationship, name, title, degree, postal address and year of birth. The respective provisions in the current draft regulation are not appropriate and therefore not supported by HDE. A general reference to all exemptions in article 6, paragraph 1 or at least an opening clause for national regulation – for example through an extension of article 21 - would be desirable.

In this context also the delegation of competences to the EU Commission in article 6, paragraph 5 which provides for the detailed definition of the application of the balance of legitimate interests clause (Art. 6 para. 1 f)) by means of a delegated legal act is problematic. Such crucial content should absolutely be included in the text of the regulation itself and in accordance with the proper legislative procedures with the full involvement of the EU Parliament.

b) Consideration of legitimate interests (article 6, paragraph 1 (f))

In comparison with directive 95/46/EG, in article 6, paragraph 1 (f) the reference to the justified interest of third parties was discarded. Even if this is not immediately obvious, this change will have massive consequences for the retail sector as it withdraws the legal basis for the work of commercial credit agencies. Credit agencies supply retail companies with credit rating information of customers which enables retailers to assess the risk of payment default before concluding a business transaction. Without this service, paying by invoice would be unthinkable – in B2C as well as B2B transactions and especially for online retail. In case of limited availability of credit checks, large mail order companies are expecting bad-debt losses of 10 million euros per year. Therefore, distance selling companies will probably limit their range of payment methods offered to customers to payment in advance, cash on delivery and credit card and would not any longer offer payment by invoice which is very popular with German consumers. Mainly consumers would have to deal with the disadvantages of this development as they would either have to pay by credit card which is costly or would be exposed to higher risk in dealing with dubious vendors when paying in advance or on delivery.

Credit agencies collect data on the payment behaviour of persons and companies. On the basis of these data they can give a factual assessment on the credit rating of an individual or a company upon receipt of an inquiry. Credit agencies collect and process data not for their own purposes but in the interest of companies which ultimately use their services.

From our point of view it is therefore imperative that article 6, paragraph 1 (f) would refer again to the justified interest of third parties in order to avoid economic damage. In this context we would like to point out that the consideration of the “interests or fundamental rights and freedoms of the data subject” is always necessary and hence the latter are already adequately protected.

c) Collective labour agreements/ company agreements

The list of permissions for the data processing should by all means be broadened in order to make sure that collective labour agreements and company agreements are also considered as a possible legal basis for processing data (see comment on article 7, paragraph 4) as long as the level of protection prescribed by the regulation or national laws is not lowered. Both instruments are negotiated in detail between legitimate employee and employer representative or work councils and should therefore be seen as a valid equivalent to regulations.

4. Conditions for consent (article 7) und employee data protection (article 82)

a) Burden of proof (article 7, paragraph 1)

Concerning the scope of the burden of proof within the context of the consent, a clarification is urgently needed from a retailers’ point of view. Does the existence of the consent have to be proven as such or does the identity of the data subject have to be proven beyond that? Furthermore, there is a lack of differentiation between the consent within the context of an individual contractual situation or the anonymous use of the internet. Can one deduce *a contrario* from article 8 that

solely the low requirements for consent of article 7 have to be met? A one-sided transfer of the burden of proof to the controller is not acceptable. This does not correspond to the objective of a balanced risk distribution.

b) Withdrawal (article 7, paragraph 3)

In certain aspects Article 7, paragraph 3 contradicts article 17. Whereas according to article 7, paragraph 3 the withdrawal of consent does not concern the legality of the data processing, according to article 17, paragraph 1 b) the data subject can nevertheless demand the erasure and blocking of the data. In our opinion this is too extensive as the data processing done in the past would become illegal. In practice, a company will cease all data processing activities when receiving a withdrawal of consent anyway. However, data collected in the past should not be subject to a global deletion obligation. For clarification in article 7, paragraph 3, sentence 1 the additional phrase “with effect from that moment and the future” should be added after “any time”.

c) Significant imbalance (article 7, paragraph 4)

According to article 7, paragraph 4 the consent of the data subject does not offer a legal basis for the processing “where there is a significant imbalance between the position of the data subject and the controller”. This limitation of the permission of data processing via consent is extremely problematic. There is hardly a situation in life where both contractual parties are on a par with each other. In case of an extremely narrow interpretation of this restriction by the supervisory authorities this could have the consequence that giving consent to data processing would be virtually impossible. In addition, this is not compatible with the principle of autonomy with regards to the handling of one’s own data and hence is very problematic. Furthermore, the regulation brings legal uncertainty as the term “imbalance” has not been defined.

As this also applies among others to employment relationships (see recital 34), we see need to significantly redraft article 7, paragraph 4. The regulation should not contain any global elimination of consent within the context of an employment relationship. Otherwise a situation could arise where employers could only process data when legally obligated to do so.

The limitation of the possibility to consent to the processing of one’s own data should therefore be eliminated or at least limited to single, enumerative listed situations which are prone to misuse.

Should this not be desirable at a political level, the question as to whether a “significant imbalance” actually is at hand should be assessed individually on a case by case basis. Otherwise it would in future be impossible to collect and process employee data by the company, e.g. within the context of a general flu vaccination initiative for employees, for the establishment of a company nursery, for an internal employee training program or for similar services for the benefit of the employees. Such legal consequences would be unbalanced and far from real life conditions and are therefore hardly acceptable. From our point of view, a differentiation should be made according to whether the position of dependence has had an influence on the concrete consent given by the data subject or alternatively whether the access to comparable contractual conditions would not– or at least not in a

reasonable manner – have been possible without consent. Only in these cases consent should not pose a legal basis for the data processing.

d) Employee data protection (article 82)

Firstly, it should be noted that generally a harmonised provision on employee data protection throughout the EU as part of this regulation would be welcome. However, this only applies if it were possible to agree on an appropriate provision for the consent in the context of employment relationships within the regulation (see explanation for article 7, paragraph 4). Moreover, it has to be ensured that collective agreements such as collective labour agreements and company agreements can form the legal basis for a data processing.

Should this not be feasible within the framework of this legislative procedure, it is necessary to include an exemption clause for labour law which would allow national legislators to take into account the particular conditions of local labour laws and avoid legal conflicts between EU data protection and national works constitution and labour law. The exemption clause as proposed by article 82 falls short of this goal. Especially the restriction "within the limits of this regulation" would have to be deleted or rather clarified in order for legislation at national level - e.g. divergent regulation for consent within the context of an employment relationship or collective agreements in labour law – to be admissible. Otherwise the exemption clause of article 82 would be obsolete.

Within this contest it is also problematic that according to article 51, paragraph 2, in future the data protection agency situated at the location of the headquarters of a company should be responsible. At the same time employee data protection is regulated at the national level and will not be harmonized (article 82). It would follow that a national data protection agency would also in future be responsible for the monitoring of the compliance with employee data protection rules in other countries. However, the practical implementation of this would most probably cause problems regarding capacities and competences.

5. Right to be forgotten (article 17)

From our point of view it is crucial to clarify within the text of the proposed regulation that the rules in article 17 are also fulfilled if the controller has anonymised or consolidated personal data. In particular this is important to advertising retail companies. Following an advertising campaign after which the storage deadline - for which consent has been given - has expired, companies should be allowed to further process information on the success of the campaign and the customer reaction in an anonymised fashion. An obligation to erase would restrict the lawful interests of the company excessively without providing any significant improvements to the privacy of the data subject.

6. Right to data portability (article 18)

Article 18 of the draft regulation obliges companies to hand over collected personal information to their customers. In our opinion these obligations are very one-sided and tailored to certain services, such as social networks or cloud computing. Obviously with these measures consumers are supposed to gain more control over this kind of data which they have submitted via the internet voluntarily. Extending this

rule to encompass the right to information (article 12 of regulation 95/46/EG) as proposed here definitely goes beyond the intended objectives. For retail companies the inclusion of such a rule on data portability would have grave consequences. In our view, a more differentiated approach is necessary in order to meet the needs of other business models whose focus is not processing data.

In the different retail formats – in e-commerce as well as in over-the-counter retail – data on customers and buying behaviour are stored. The legal basis for this is the consent of the person or a contract. Prevalent examples of this are customer cards which retail companies use to increase customer loyalty and to address their customers more effectively. These data which have been collected by the companies over a certain period of time have a significant value for the company and therefore represent an economic commodity as they allow a company to gain important insights into the preferences of its customers. For the purchasing and the determination of the variety of a company's product range, the preparation of measures to increase customer loyalty (e.g. price discounts) as well as for the planning of advertising campaigns this type of data are essential.
From our point of view the obligation of companies to reveal these data goes too far and cannot be justified with the protection of the privacy of data subjects. Completely unacceptable is the requirement that companies should have to "transmit those personal data […] retained by an automated processing system, into another one, in an electronic format which is commonly used". Regardless of the resulting loss in value for the company, this measure would pose a significant competitive disadvantage would these data be passed on to competitors.

To avoid economic damage as detailed above article 18 should be limited to those services which allow consumers the publication of their personal data. In all other situations, the right of the data subject for protection of their personal data is sufficiently protected through the limitation of the legality of processing (article 6), the right to information (article 15) and the right to objection (article 19). Alternatively, a differentiation with regards to the type of data would be necessary. Solely information which was provided voluntarily and on one's own initiative ("user generated content") should fall within the scope of the right to data portability – however not operative data sets which have been systemically analysed by companies.

7. Bureaucratic burden

The retail sector explicitly welcomes the aim to reduce bureaucratic burden. Even though in the regulation proposal several rules have been eliminated compared to the existing data protection directive (especially the notification requirement in article 18 of directive 95/46/EG), new obligations have been introduced in other areas which in fact could result in an additional burden for companies.

a) Burden of proof (article 5 (f))

From a retail perspective the burden of proof as outlined in article 5 f) regarding the compliance with the rules of the regulation is problematic as it would result in considerable administrative burdens. Compared to the liability for the order processing or the proof that action was taken in accordance with due diligence principle, this global obligation to produce supporting documents seems inappropriate. In its proposed form this obligation to provide proof is hardly practicable as it is neither specified in which manner this proof should be provided nor to whom the con-

troller should provide it. Within the text duplication should be avoided. Detailed rules for a satisfactory degree of transparency and accountability have been established with the information obligations (article 14) and the right to information (article 15). Therefore the rather abstract burden of proof in article 5 (f) should be eliminated.

b) Development of a data protection policy (article 11)

It is still unclear what is meant by “data protection policy”. Recital 61 mentions “internal policies”. For companies the question is therefore whether in future they have to ensure that their internal strategies are “easily accessible”? Here it should be clarified that under no circumstances IT security features or business secrets should have to be published. One option would be to differentiate between public and internal registers of processing operations which is missing so far.

The regulation proposal does not suggest how highly complex sequenced within data processing can be communicated in “an intelligible form, using clear and plain language, adapted to the data subject”. For companies this clearly poses the risk to be reprimanded under competition and consumer protection legislation in case they describe their data processing sequences in a simplified manner (i.e. suitable for consumers) but do not convey the whole complexity of it. In this context it is not helpful that according to article 11, paragraph 2, “any information and any communication relating to the processing of personal data“ have to be made available. This contradicts the objective to present the information in a language that is clear and suitable for the audience. A list of elements which should be transmitted to the data subject for reasons of transparency would be helpful.

c) Information obligation (article 14)

With regards to the obligation to declare the duration of the storage of personal data according to article 14, paragraph 1 c), it should be clearly stated that this is not necessarily be done by stating a date. In practice not in all cases is an end date for the contractual relationship fixed when starting data processing. This rule has to have flexibility as an extensive limitation would drastically affect internal organisational processes of a company.

In order to simplify this article, changing the wording of paragraph 5 a) by substituting the phrase “referred to in paragraphs 1, 2 and 3“ with the words „knowledge of storage or transmission of date“ would make sense.

d) Right of access (article 15)

In our opinion the comprehensive global right of access regulated in article 15 has to be supplemented with a proportionality clause. We believe that a time limitation should be foreseen which clearly defines in which time intervals information can be demanded (e.g. once per calendar year) in order to ensure proportionality and prevent abuse.

Furthermore, article 15, paragraph 4 is questionable as far as it states that the EU Commission can set standard templates for information access. This would interfere considerably with the particular organisational structure of a company.

8. Responsibilities for the controller (article 22 and the following)

a) Obligation to keep records (article 22, paragraph 1; paragraph 28)

The intended general burden of proof of article 11, paragraph 1 is too global and would result in significant bureaucratic burden and increased costs.

Also the obligation to keep records of article 28 is too extensive. In our view, the obligation to keep records as defined by the German Data Protection Act would be sufficient (§ 4 g) para. 2 with § 4 d) and § 4e) BDSG).

With regards to article 28, paragraph 4 b), it should generally be noted that not solely the total number of employees should be taken into account but rather the number of employees whose work relates to data protection aspects.

b) Notification of a personal data breach (article 31, 32)

The intended notification obligation in case of data breach is too global and from our point of view hardly implementable. The notification obligation should be limited to serious breaches within a limited time period. (cfr. § 42 a) BDSG).

The current proposal is problematic in two ways. Firstly, it lacks a limitation on the notification obligation to serious breaches or a differentiation between serious (for sensitive data) and bagatelle-type breaches of data protection. Secondly, the proposed notification obligation within 24 hours is too rigid. It seems that an attempt has been made to introduce flexibility with the phrase “where feasible” as well as article 31, paragraph 1, sentence 2. However, in our opinion this is not sufficient as “where feasible” is an extremely vague term and deviating from the 24 hour deadline will go hand in hand with an obligation to give an explanation. Overall, the proposed regulation would mean that companies have to notify even less serious cases of breach within 24 hours which poses an enormous organisational and financial challenge. It would be preferable to eliminate the 24 hour deadline and substitute it with a term such as “within an adequate period of time”.

c) Obligation for prior authorisation (article 34)

The obligation according to article 34 - which states that for data processing prior authorization is needed or the advice of a governing body has to be sought – has to be clarified. It is unclear whether an obligation to obtain authorisation according to article 34, paragraph 1 applies to all data processing sequences or whether this is limited to the mentioned cases (contractual clause according to article 42, paragraph 2 d or lack of guarantee according to article 42, paragraph 5). According to our understanding the latter is the case which however is unfortunately not obvious from the wording. Additionally, one has to point out the inconsistencies of the different language version (English-German). An authorisation obligation which is too general would result in significant additional bureaucratic burdens and accordingly data processing sequences would take considerably longer. This would hinder the competitiveness of the fast and straightforward processes of mail-order or online retailers. Moreover, the undefined legal terms in article 34, paragraphs 2 a) and b) do not contribute to legal certainty. For example, it is unclear in which cases the processing sequences are of “high” concrete risk as defined by paragraph 2 a). Moreover, it is questionable whether 27 national lists of processing sequences as described in article 34, paragraph 2 b) compared to paragraph 4 could help here. A corresponding revision of the text which states this issue unambiguously is

urgently needed from our point of view. In our opinion the notification obligation to the authorities should be omitted as soon as a data protection official is appointed. (cfr. § 4d) para. 2 BDSG).

d) Data protection officer (article 35)

The self-regulation approach of appointing a data protection officer as described in article 35 is welcomed. It offers the opportunity to establish data protection officers, which have been successful in German legislation, throughout the EU. Generally we have doubts whether the amount of employees an indeed be indicative of the potential data protection risks of a company. Should this criterion of the number of staff be kept, we believe that there is a need to improve the definition of "employee" and the threshold value foreseen. It should be clarified whether self-employed employees are to be be included in this figure. Secondly, the number of mentioned employees should solely include those who actually work in the area of data processing. Only in this manner, the companies who not only carry out data processing on a large scale will actually be included and an efficient use of the function of data protection officer could be achieved.

9. Profiling (article 20)

In connection with article 20, a greater amount of legal certainty should be created by defining the term „profiling" in article 4. In such way, misunderstandings with regards to profile generation – which is often termed "profiling" - could be prevented.

From the retail sector's point of view article 20, paragraph 1 (at the end) is extremely problematic. With it, internal credit worthiness checks and estimates of credit default risk for invoice and instalment purchases ("economic situation") would be impossible in future. As a result customers would only be able to pay by secure means of payment. Should credit checks only be possible with the customer's consent in future, large mail order retailers are expecting significant monetary effects of up to 10 million euros of bad debts per year.

In our opinion the empowerment of the Commission in article 20, paragraph 5 by means of delegated legal acts to further limit article 20, paragraph 2 is alarming as this causes considerable legal uncertainty.

10. Video surveillance (article 33, paragraph 2c)

From a retail perspective one-sided regulations on video surveillance should generally be avoided. Video surveillance is an important instrument to guarantee the security of employees and the company property as well as to prevent criminal offences. It is important to stress in this context that surveillance is solely used for prevention purposes, not for obtaining employee data.

Article 33, paragraph 2 c) authorises video surveillance – on the condition that an impact assessment has been carried out previously. In this context the following aspects are of concern for the retail sector:
For a start the scope of the term "publicly accessible areas" has not been defined. Does this include only public spaces and building or does it also apply to privately owned shops which have been opened to customers?

In the latter case the obligations described in article 33, paragraph 4 for consultation of the affected persons or their representatives prior to video surveillance is problematic. It remains unclear who in particular cases the “representatives” of the affected persons would be. Moreover, such a general consultation obligation would be disproportionate should it be interpreted in such way that possibly every single customer has to be consulted prior to video surveillance for the purpose of crime prevention. This would be completely unfeasible. The monitoring of the supervisory authorities and the company data protection officer in combination with an impact assessment should in this case be sufficient to protect the right of the affected persons.

With regard to the working conditions a consultation should not be necessary as already the work councils have to agree to video surveillance according to national labour constitution legislation. It remains to be considered whether it would not be sensible at this point to refer to article 82 of the regulation proposal for employment protection related constellations.

11. Enforcement (article 73 and following, especially article 76)

In our opining the possibility for class actions as described in article 73 is unnecessary. The data protection authorities are obliged to accept and investigate complaints of data subjects. They already have sufficient corrective instruments at their disposal as they are authorised to order corrective measures (article 53, paragraph 1). Therefore problems are usually solved at the level of the data protection authority. Hence, the introduction of a second, competing corrective instrument does not make sense.
Apart from that there is a lack of safeguards in order to avoid cases of abuse. Here especially the introduction of a bagatelle threshold as well as a clear definition of organisations with legal standing would be necessary.

12. Sanctions (article 78 and following)

Sanctions or penalties linked to the annual turnover would jeopardise the existence of companies in low-margin sectors such as retail (usually between 0.5% – 2%) as well as companies whose business model is not based on data processing and are therefore unacceptable.

It is moreover problematic that the regulatory authorities hardly have the possibility for discretionary decisions when imposing sanctions. On the contrary, there is an obligation according to article 79 to impose sanctions when an offence is presented. Against this background, the introduction of a bagatelle threshold is advisable. It is also not comprehensible why a written warning should not represent a “sanction”.

Alternatively, an entitlement to skimming of profits could be a solution in which the profit would replace the turnover as decisive value in the calculation of the sanctions.

Furthermore, the transfer of powers to the EU Commission by means of delegated legal acts for updating amounts of penalties is seen with great concern.

13. Data transfer within corporations

Concerning data transfer into third countries and international organisations as mentioned in article 43, we plead for the introduction of a so-called “corporate privilege” into the proposal, i.e. a regulation which enables the transmission of data to subsidiary companies within a corporation without the need for separate contractual agreements.

The current legal situation treats the transmission of personal data within the corporation to subsidiary companies as transfer to third parties. This calls for complex corporate guidelines and data processing contracts between subsidiary companies which are cumbersome and impractical. A corporation is an economically united structure which – regardless of the independence of the companies – makes a centrally organized data processing and other issues bundled for the whole corporation possible and sensible with regards to efficiency.

Berlin / Brussels, September 2012