verbraucherzentrale
Bundesverband

29 July 2015

# EUROPEAN DATA PROTECTION LEGISLATION MUST MEET DIGITALISATION CHALLENGES

**Ten core positions of the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband)**

on the trilogue negotiations 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)


**Masthead**

*Verbraucherzentrale*

*Bundesverband e.V.*

*Markgrafenstrasse 66*

*10969 Berlin*

## I. Introduction

Digitalisation influences and changes all spheres of people's lives. There are quite a few everyday activities today that can hardly be done without access to, and use of, the Internet. Interconnected devices, while simplifying consumers' lives, keep generating data, leave lasting traces of data behind, and combine data into the most varied statements and forecasts that cannot be controlled individually. The previous European Data Protection Directive of 1995 (95/46/EC) does not cover many of the data protection questions which consumers are facing today. Modernising the legislation by adjusting it to the challenges of digitalisation is therefore an urgent requirement to ensure that personal data and the consumers' privacy will be protected in the future and, at the same time, to strengthen legal certainty and competitiveness of European enterprises.

The General Data Protection Regulation of the European Union (EU) therefore is one of the most important regulatory instruments for the years, if not the decades, ahead. Verbraucherzentrale Bundesverband (vzbv) therefore welcomes the fact that, after the European Parliament, the Council of the European Union has now, three and a half years after the draft regulation was presented by the European Commission, taken a position and made it possible for the trilogue negotiations to start. The vzbv supports the declared goal to conclude these negotiations by the end of 2015.

In the opinion of vzbv, it is regrettable that the discussion has gradually moved into a direction less favourable to data protection in the past three years. While the European Commission had rightly promised its EU citizens to increase the level of data protection and presented a consumer-friendly proposal which was further strengthened by the European Parliament, the clearly more business-friendly position taken by the Council of the European Union has created a situation for the trilogue negotiations in which just maintaining the level of the previous regulations of the 1995 Directive and national regulations might be negotiated. This jeopardises the overall goal of an urgent modernisation of the 1995 Directive.

The vzbv therefore urgently appeals to all institutions of the European Union and to the Member States to consistently place the rights of their citizens as consumers in the forefront of designing the General Data Protection Regulation and to keep their eyes on the declared goal: To strengthen informational self-determination of citizens and consumers. This goal also enhances the competitiveness of the European economy. In the future, those enterprises will stay ahead which handle the raw material of the digital world – the data – in a responsible and trustworthy manner. It is therefore important that individuals and their right of sovereignty over their data is made the starting point of considerations regarding the design of data protection, especially in a world that is becoming more and more digital.

## II. Summary of positions

### 1. Personal data and pseudonymisation

The vzbv supports the positions taken by the **European Parliament**, according to which the principles of data protection shall apply to all information – including pseudonymous identifiers – which can be used to directly or indirectly identify or single out a person.

### 2. Consent

The vzbv supports the proposal by the **European Commission** and the position taken by the **European Parliament**, according to which consent should be a freely given, specific, informed and explicit indication by which the data subject signifies agreement to personal data relating to them being processed.

### 3. Data minimisation

The vzbv supports the endeavours by the **European Commission** and the **European Parliament** to further develop data protection based on its current principles, in particular, the principle of data minimisation. Otherwise, the new regulations would fall short of existing standards.

### 4. "Legitimate interest" of the data controller

The vzbv criticises that neither the European Commission nor the European Parliament or the Council of the European Union have defined clear criteria for a narrow interpretation of "legitimate interest". The vzbv further criticises that the planned regulations fall short of the German Federal Data Protection Act and state that direct marketing is in general a "legitimate interest" of the data controller. In view of the existing positions, vzbv prefers the position taken by the **European Parliament,** because its proposed regulations provide the strongest protection of the data subjects for data processing based on a "legitimate interest".

### 5. Change in the purpose of processing

The vzbv supports the position taken by the **European Parliament**, which removed some critical wording of the draft presented by the European Commission that would have allowed a change in the purpose of processing even if the further processing was incompatible with the purpose for which the personal data have been collected. The new regulation should not fall below the level of protection provided in the EU Charter of Fundamental Rights and Directive 95/46/EC.

### 6. Processing children's personal data

The vzbv supports the **European Parliament's** position that the processing of personal data of a child below the age of 13, to whom goods and services are offered directly, should only be legitimate if consent is given or authorised by the child's parent or legal guardian.

### 7. Information of users / right to information

The vzbv welcomes the positions taken by the **European Parliament** which provide for a layered but nonetheless sufficiently detailed system for informing consumers and letting them exercise their rights of information.

### 8. Right to data portability

The vzbv endorses the positions taken by the **European Parliament**, which grant a broad right of data portability, prevent that the data controller can prevent data subjects from exercising their right and emphasize that data must be deleted by the controller when the purpose of storage is eliminated by data transfer.

### 9. Profiling

The vzbv thinks that only the positions taken by the **European Parliament**, which clearly define profiling, cover every form of profiling, grant the data subject the right to object profiling and preserve the fundamental right of informational self-determination.

### 10. Right of associations to take legal action

The vzbv endorses the positions taken by the **Council of the European Union** according to which an organisation, independently of a data subject's mandate, has the right to lodge a complaint and to exercise the data subject's rights if it considers that the rights of a data subject have been infringed as a result of the processing of personal data that is not in compliance with the Regulation. However, this option to exercise the data subject's rights independently of a data subject's mandate should be introduced as a binding clause in all Member States in the spirit of applying the same regulations throughout the EU.

## III. The positions in detail

### 1. Personal data and pseudonymisation

Pseudonymisation is a means to temporarily separate data from its reference to a person. This can reduce risks for the data subjects, for example, by restricting access to personal data, their analysability, and the number of individuals who have access privileges. Pseudonymisation therefore is a building block for implementing the principle of data minimisation.

The pseudonymous files will however still be personal data (this is what differentiates pseudonymisation from anonymisation). Pseudonymised data that cannot be directly assigned to individuals may still result in individual impairments. This data allows to single out individuals and subject them to a different treatment. Therefore, the regulation should fully include pseudonymous data as well.

To protect consumers' rights appropriately, it should be made clear that ID numbers, location data, online identifiers or other similar pseudonymous elements are always personal data if they can help to determine a person. The regulations should also be kept technology-neutral and not be limited to online services and identifiers, so as to include offline techniques such as the use of RFID in the end customer sphere.

**The vzbv supports the positions taken by the European Parliament (Recitals 23, 24; Article 4.2), according to which the principles of data protection shall apply to all information – including pseudonymous identifiers – which can be used to directly or indirectly identify or single out a person.**

### 2. Consent

Consent of a data subject to personal data processing is a critical element of the fundamental right to informational self-determination. The respective provisions must be worded clearly. The previous provisions and the respective current proposals, according to which consent must be given unambiguously, lack such clarity. For example, this wording has been interpreted in the past to mean that the mere use of a website or service was consent to the use of a person's data. It should be made clear that consent must be given explicitly in the future and that implicit consent without active participation of the data subject is excluded.

**The vzbv supports the proposal by the European Commission (Article 4.8) and the position taken by the European Parliament (Article 4.8), according to which consent should be a freely given,**

**specific, informed and explicit indication by which the data subject, signifies agreement to personal data relating to them being processed.**

**In principle, vzbv welcomes the position taken by the Council of the European Union (Recital 25), according to which consent can be given by using the appropriate settings of a web browser or another application, *with the proviso that the web browser or other applications comes with a default setting at delivery that does not express consent (privacy by default)*.**

It is imperative that such consent must be freely given. Specifically, this requires provisions regarding the prohibition of coupling. Prohibition of coupling means the provision of a service shall not be made conditional on the consent to the processing of personal data that is not necessary for the provision of the service. This type of coupling is contrary to the principle of free consent and must be prevented.

**The vzbv supports the positions taken by the European Parliament (Recital 33; Article 7.4), according to which the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the provision of the service.**

### 3. Data minimisation

Data minimisation is a basic principle of data protection. The German Federal Data Protection Act stipulates, for example: *"Personal data are to be collected, processed and used, and processing systems are to be designed in accordance with the aim of collecting, processing and using as little personal data as possible."*

This is to reduce the risks of data processing and to maintain its adequacy. Companies must therefore always critically review if the data to be processed is really required or if the same purpose can be achieved with less (or pseudonymised or anonymised) data. This promotes the development and use of privacy-friendly technologies.

According to the proposals made by the Council of the European Union, data processing would no longer have to be limited to a minimum but just be "not excessive". This would mean a clear reduction of the current level of data protection. This proposal by the Council is therefore unacceptable.

**The vzbv supports the endeavours by the European Commission (Article 5c) and the European Parliament (Article 5c) to further develop data protection based on its current principles, in particular, the principle of data minimisation. *Otherwise, the regulations would fall short of the existing ones. There must be no compromises here.***

### 4. "Legitimate interest" of the data controller

The legitimacy of processing can be based on the "legitimate interests" of a data controller except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. But the provision must not become a catch-all reason for processing which the data controller just does not want to justify on other potential legal grounds. Accordingly, data processing should only be allowed based on balancing interests if such processing is actually required for objective reasons (which in general can't be taken for granted for advertising purposes).

The vzbv deems it imperative that the regulation will not allow a broad interpretation of "legitimate interest", especially since the Council of the European Union demands that a change of the purpose of processing should also be permitted based on balancing of interests, even if is incompatible with the one for which the personal data have been collected. If the "legitimate interest" of enterprises is interpreted too broadly, purpose limitation would practically be eliminated.

Before this background, vzbv critically notes that the European Parliament and the Council of the European Union view data processing for the purpose of direct marketing as generally covered by the "legitimate interest" of the data controller or a third party to whom the data was transferred. These positions even fall behind the regulations that are currently applicable in Germany.

The vzbv therefore criticises that neither the European Commission nor the European Parliament nor the Council of the European Union have defined clear criteria for a narrow interpretation of "legitimate interest". The consent of the data subject should have to be obtained in general for the use of personal data for direct marketing purposes.

**All wordings proposed are unsatisfactory in the opinion of vzbv. In view of the existing positions, vzbv prefers the position taken by the European Parliament (Recital 38 – 39b, Articles 6.1f., Article 19.2), because its proposed regulations provide the strongest protection of the data subjects for data processing based on a "legitimate interest".**

### 5. Change in the purpose of processing

The principle of purpose limitation is one of the pillars of data protection. It is enshrined in the EU Charter of Fundamental Rights, according to which data may only "*be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law*". The European Data Protection Directive 95/46/EC provides that personal data may only be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*".

The draft by the European Commission introduces a provision contrary to this, according to which personal data may be further processed even if the purpose is incompatible with the one for which the personal data have been collected if another justification, such as consent or a contractual basis is relevant. In its position, the Council of the European Union goes even further and advocates an extension of the provision to personal data that is processed based on a "legitimate interest". This would eliminate the purpose limitation, in particular in conjunction with the broad interpretation of the term "legitimate interest" in the regulation.

The vzbv generally rejects any further processing of personal data that is not compatible with the purpose for which the personal data have been collected. Such a provision gives too much leeway to data controllers wishing to further process the data and to transfer it on to third parties. It will inevitably result in consumers having to face further utilisation of their data unexpectedly. This will destroy the consumers' trust that businesses will handle their data responsibly and according to their wishes. Justified trust will require clear legal boundaries of data processing as well as a strict principle purpose limitation.

**The vzbv supports the position taken by the European Parliament, which removed some critical wording of the draft presented by the European Commission (Article 6.4) that would have allowed a change in the purpose of processing even if the further processing was incompatible with the purpose for which the personal data have been collected. *The new regulation should not fall below the level of protection provided in the EU Charter of Fundamental Rights and Directive 95/46/EC.***

### 6. Processing children's personal data

Due to their special need for protection, children's personal data should be subject to special restrictions. It should be made clear that all individuals blow the age of 18 years are to be considered as children.

**The vzbv supports the proposal by the European Commission (Article 4.18) and the position of the European Parliament (Article 4.18), according to which a "child" means any person below the age of 18 years.**

The younger the children are, the less they are capable of assessing if the disclosure of their data is legitimate, required and useful, and the less they are capable of seeing and correctly assessing the consequences of the use of their data. For these reasons, especially younger children should not be able to consent to data processing themselves – the European Commission, the European Parliament and the Council of the European Union agree in this respect. However, it is necessary to define an age limit after which children may themselves give their consent to the processing of their personal data. The vzbv considers an age limit of 13 years of age as the absolute minimum.

Furthermore, these provisions should not be limited to situations in which children under 13 years of age are offered "information society services"; instead, they should also apply to offers of goods or services of any kind.

**The vzbv supports the European Parliament's position (Article 8.1) that the processing of personal data of a child below the age of 13, to whom goods and services are offered directly, should only be legitimate if consent is given or authorised by the child's parent or legal guardian.**

Furthermore, the collection of data from minors should be subject to special restrictions that cannot be revoked by consent. For example, the profiling of minors should be excluded in principle due to their increased need for protection in proportion to the depth of intervention in individual rights such profiling constitutes.

**The vzbv welcomes the proposal by the European Commission (Recital 58) and the respective position taken by the European Parliament (Recital 58) according to which minors should be generally excluded from profiling. *But these provisions should also be included in Article 8.***

### 7. Information of users / right to information

The vzbv agrees that transparency is a fundamental prerequisite for sovereignty of the individual over his or her data and for effective data protection. It is important for the data subject to be able to evaluate the data processing before

giving his or her consent or even concluding a contract that this information is made available before the first data collection (if the data is collected from the data subject), promptly (if the data is not collected from the data subject), but at any rate before any transfer or use of the data.

The vzbv advocates a layered information system with which the information can be provided in a comprehensible form and in a manner and volume that is adequate for the context. In a first step, simplified information, e.g. using icons or pictograms, should be presented in such a system. In a second stage, the consumer should receive basic information about the data controller, the purposes of data processing, the general origin of the data, the categories of potential recipients, possible data transfers to third countries and the consumer's other rights. Information provided to the data subject upon request in the third stage should be the most detailed. For example, a data subject should not just have to be informed about categories of the data processed or categories of recipients of personal data but always about the exact data and their source and the exact recipients of the data. Only in this way can the data subject exercise his or her rights vis-a-vis these recipients.

**The vzbv welcomes the positions taken by the European Parliament (Articles 13a, 14, 15.1) which provide for a layered but nonetheless sufficiently detailed system for informing consumers and letting them exercise their rights on information.**

The vzbv does not consider it the right path to adjust the rights a data subject can exercise to the supposed risk of data processing. While such a risk-based approach can be useful when shaping the detailed technical and organisational data protection measures, the rights granted to the data subject should always be exercisable regardless of the level of risk involved. The vzbv therefore rejects the wording provided by the Council of the European Union which would leave it to the enterprises which information they provide to the data subject "taking into account the particular circumstances and general conditions". Such wording creates too much leeway for interpretation, contributes to uncertainty, and would inevitably reduce the level of protection for the data subjects.

### 8. Right to data portability

The proposal to introduce a right on data portability is welcomed because it strengthens the consumers' control over their data. The easier it is for a consumer to switch services, the less consumers will feel bound to this service, especially if they are unhappy with this service or have to subject to changes in the general terms and conditions of the service or new rules in data protection policies. This promotes competition in the market and reduces market

dominating positions of enterprises. Data protection could thus become a genuine competitive factor which helps new enterprises to shape their profiles without being thwarted by lock-in and network effects of the market leaders.

However, the focus of this provision should not be restricted to data processing based on consent; it should also be applicable to data processing based on contractual obligations.

In addition, the right to data portability should not be restricted to data that is available to the data controller in a "commonly used structured format". Otherwise, the data controllers could shirk their responsibility by using uncommon formats. To close this loophole, it must be made clear that the data provided to the data subjects must be interoperable. In addition, the data controller must not obstruct the user by not offering any (technical) ways of transfer. It should also become clear that the data controller must delete the data if the purpose of storage is eliminated by its transfer.

**The vzbv endorses the positions taken by the European Parliament (Article 15.2), which grant a broad right to data portability, prevent that the data controller can prevent data subjects from exercising their right and emphasize that data must be deleted at the controller when the purpose of storage is eliminated by data transfer.**

### 9. Profiling

Increasing digitalisation systematically results in the collection of more and more information about preferences, views and personal circumstances of consumers and their combination in profiles. The goal is to be able to predict and thus to control human behaviour. Data that provide detailed information about motivations, preferences, relationships, health or other factors influencing a person's self-worth have become valuable marketable commodities. Such data can be critical for decisions if consumers are granted loans, what insurance premiums they must pay or what prices they pay for goods. Profiling thus does not just have a massive impact on an individual but on society as a whole. It is all the more important that profiling should be consumer-friendly with clearly defined boundaries.

This means that regulations should not just include decisions that are based on profiling; they should also limit profiling itself. The mere creation of a profile deeply intervenes in the rights of the data subject. Profiling should not only regulated when it produces legal effects concerning this consumer or significantly affects him. Otherwise, profiling in order to display individualised ads to consumers or to offer products and services at individualised prices would not be covered by the regulation at all.

**The vzbv thinks that only the positions taken by the European Parliament, which clearly define profiling (Article 4.3a), cover every form of profiling (Recital 24), grant the data subject the right to object profiling (Article 20.1) and preserve the fundamental right of informational self-determination**.

Processing of special categories of personal data is particularly critical with respect to profiling. Therefore, profiling based on special categories of personal data should only be permissible under strict conditions.

***With the proviso that the rule does not just relate to decisions based on profiling and produces legal effects concerning this consumer or significantly affects him, but to any form of profile creation as such*, vzbv welcomes the position taken by the Council of the European Union (Article 20.3), according to which the processing of special categories of personal data is permitted under narrow conditions only.**

The vzbv rejects the position taken by the European Parliament which assumes that the creation of a profile that is only based on analysing pseudonymous data in general has no significant effect on the interests, rights or freedoms of a data subject. Since pseudonymous data is personal data, pseudonymous profiles allow that individuals are singled out based on these profiles. For example, information contents, offers or prices can be individualised based on these profiles. It often makes no practical difference to the data subject if a profile that applies to him or her was created under a pseudonym or under his or her real name.

### 10. Right of associations to take legal action

Consumer protection associations have noticed an increasing number of breaches of data protection regulations in recent years. However, many consumers are not in a position to enforce their claims against enterprises successfully, if required, by going to court. The negative effects are often too difficult to prove for an individual that it would be useful to accept the effort and cost of lengthy court proceedings against, for example, an international group of companies. Nonetheless, many of these breaches are mass phenomena which affect large numbers of consumers. This is where collective legal protection must come in: An association entitled to take legal action will make sure in the interests of the consumers that breaches of the law are stopped. Initiating a single injunction procedure can efficiently and cost-effectively prevent other abuses of the law, for example, because the court will settle an uncertain legal situation.

The vzbv therefore welcomes the fact that organisations that represent the interests of data subjects will in the future have the right to file a complaint against violations of data protection with the supervisory authority or take legal action against enterprises. This relieves the burden of the supervisory authorities, strengthens the enforcement of consumers' rights and helps to create legal certainty for all enterprises. In order to ensure a high level of data protection and provide the best legal basis for exercising and protecting collective interests, data protection and consumer associations should not just be granted an indirect right to take legal action (i.e. after claims were assigned to them or they received a mandate), but an original/direct right to take legal action (independently of a mandate by a data subject).

Furthermore, the regulation should not rule out that institutions, organisations or associations can demand compensation for damages on behalf of data subjects based on national law.

**The vzbv endorses the positions taken by the Council of the European Union (Recital 112, Article 76.2), according to which an organisation, independently of a data subject's mandate, has the right to lodge a complaint and to exercise the data subject's rights if it considers that the rights of a data subject have been infringed as a result of the processing of personal data that is not in compliance with the Regulation. *However, this option to exercise the data subject's rights independently of a data subject's mandate should be introduced as a binding clause in all Member States in the spirit of applying the same regulations throughout the EU.***