Bitkom represents more than 2,300 companies in the digital sector, including 1,500 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. Comprising 1,000 small and medium-sized businesses as well as 300 start-ups and nearly all global players, Bitkom' members offer a wide range of software technologies, IT-services, and telecommunications or internet services. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 78 percent of the companies' head-quarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focusing the modernization of the education sector and a future-oriented network policy.

Overview

Article 5 Principles **3**

Article 5 b) Scientific, statistical or historical purposes 3

Article 5 c) Data Minimisation 4

Article 6 Lawfulness of processing **4**

Consent - Article 6 (1) a) in connection with Article 4 (8) and Article 7 ..... **4**

Article 6 (1) a) and Recital 25 Legal basis of consent 5

Article 7 (1) and Recital 32 – Conditions of Consent 5

Article 7 (2) – Using clear and plain language 6

Article 7 (4), Recital 34 Clear imbalance 6

Article 6 (1) c) and Recital 36 Processing for compliance with a legal obligation 8

Legitimate interest clause and Pseudonymization **9**

Article 6 (1) f), Recital 38 – Legitimate interest of third parties & reasonable expectations 9

Article 6 (3) – Harmonization 11

Defining Anonymization and Pseudonymisation – Art. 4 and Recitals **12**

Article 6 (1) g) - new proposal 13

Article 6 (1) h) – new proposal 13

Recitals 38 and 58a - Pseudonymisation 14

Article 6(4) and Recitals - Further processing **15**

Article 8 (1) – Processing of personal data of a child **16**

Article 9 - Processing of special categories of data **17**

Article 10 - Processing not allowing identification **17**

Article 5 Principles

Article 5 b) Scientific, statistical or historical purposes

EP Version Article 5 b)	Council Version Article 5 b)	Bitkom
Personal data shall be: b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (purpose limitation);	b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of personal data for archiving purposes in the public interest or scientific, statistical or historical purposes shall in accordance with Article 83 not be considered incompatible with the initial purposes.	Bitkom supports the Council`s amendment as it is helpful to clarify what can be seen as compatible with the original purpose.

Commission Version Recital 40	Parliament Version Recital 40	Council Version Recital 40	Bitkom
40) The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes. Where the other purpose is not compatible with the initial one for which the data are collected, the controller should obtain the consent of the data subject for this other purpose or should base the processing on another legitimate ground for lawful processing, in particular where provided by Union law or the law of the Member State to which the controller is subject. In any case, the application of the principles set out by this Regulation and in particular the information of the data subject on those other purposes should be ensured.	**Deleted**	40) The processing of personal data for other purposes than the purposes for which the data have been initially collected should be only allowed where the processing is compatible with those purposes for which the data have been initially collected. (…) (…)	The clarification of the Commission to base processing for incompatible purposes either on consent or "another ground for lawful processing", which refers to all legal bases in Article 6, is important for understanding and should be kept. It could be moved to Art. 5 (1) (b).

Article 5 c) Data Minimisation

The current data protection regime tries to prevent the misuse of data by already restricting the collection of data (processing of data is generally prohibited unless authorized). However, Big Data, Internet of Things, Industry 4.0, E-health, E-energy, etc., which the Commission intents to foster with its Digital Single Market Strategy, will all be based on the processing of (partly personal) data and to in order to succeed they will require more, not less data.

Example Big Data: *Only with large data sets containing a variety of data types new patterns, unknown correlations, market trends, customer trends and other useful information can be uncovered.*

Bitkom supports technical data protection such as 'privacy by design' and 'privacy by default', which are often linked to the concept of "data minimisation". Furthermore, we encourage policy makers to integrate and incentivize privacy-friendly methods like anonymisation and pseudonymisation in the GDPR which are both essential for innovative business models. Nevertheless, we caution against the phrase "data must be limited to the minimum" and the tag "data minimization" as it is misleading in a data-driven society and economy.

EP Version Article 5 c)	Council Version Article 5 c)	Bitkom
Personal data shall be: c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;	c) adequate, relevant, and not excessive in relation to the purposes for which they are processes	Bitkom supports the wording of the Council which also adopts the language "not excessive" from the current Directive in Art. 6 (1) (c).

Article 6 Lawfulness of processing

Consent - Article 6 (1) a) in connection with Article 4 (8) and Article 7

The Commission and the EP demand, in contrast to the current Directive, that consent needs to be explicit (see definition in Article 4 (8). This One-Size-Fits-All requirement does not take into account in which context, e.g. technical circumstances, consent was obtained and which risks are inherent.

Example: *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 behavior must be not tracked with cookies or any other technical gadgets, or that the use of such technical tool is desired.*

Example: *Another possibility for an implicit consent is the receipt of information of a navigation system on a 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.*

Article 6 (1) a) and Recital 25 - Legal basis of consent

EP Version Article 6 (1) (a)	Council Version Article 6 (1) (a)	Bitkom
Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given consent to the processing of their personal data for one or more specific purposes;	Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: a) the data subject has given unambiguous consent to the processing of their personal data for one or more specific purposes	The Council text and the wording of the current Directive should be maintained where it is also stated in Article 7 (1): "the data subject has unambiguously given his consent".

EP Version Recital 25	Council Version Recital 25	Bitkom
(25) Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action that is the result of choice by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data. Clear affirmative action could include ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, mere use of a service or inactivity should therefore not constitute consent. (...).	(25) Consent should be given unambiguously by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a written statement, including electronic, oral statement or, if required by specific circumstances, by any other ~~clear affirmative action~~ by the data subject, signifying his or her agreement to personal data relating to him or her being processed. This could include–ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. ~~Silence or inactivity should therefore not constitute consent.~~ (...)	Bitkom supports the Council version of Article 6 (1) regarding 'unambiguous consent'. To allow for such an approach, the text "clear affirmative action" and "silence or inactivity should therefore not constitute consent'" should be reconsidered in light of cases of implicit consent or pseudonymous data.

Article 7 (1) and Recital 32 – Conditions of Consent

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 prove given consent. Already now companies usually have to prove 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 prove a filed consent, the burden of proof should be on the data subject. The possibilities of anonymized usage of internet service should not lead to a one-sided disadvantage for the controller. Furthermore, the relationship between Art. 7 (1) and Art. 10 is unclear as Art. 10 provides that the controller should not have to collect additional data merely for the purpose of complying with provisions of the Regulation.

EP Version Article 7 (1)	Council Version Article 7 (1)	Bitkom
1. Where processing is based on consent, the controller shall	1. Where Article 6(1) (a) applies the controller shall be able to demonstrate that unambiguous consent was given by the	Bitkom believes that the current model should be preserved,

bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes	data subject. 1a. Where article 9(2) (a) applies, the controller shall be able to demonstrate that explicit consent was given by the data subject.	according to which the data subjects have the right to object on the basis of compelling legitimate grounds relating to a particular process and it is incumbent on the data subject to demonstrate those ground.

Article 7 (2) – Using clear and plain language

Even though Bitkom supports the intention of the wording, "clear and plain" language, the requirement will be difficult to fulfil in practice.

Example: *For a privacy policy (e.g. laid down in terms and conditions) to be actually transparent, the policy needs to be detailed and point out exactly who interacts with the data, when, how and to what end. These details automatically render the texts complex for an average consumer.*

EP Version Article 7 (2)	Council Version Article 7 (2)	Bitkom
2. If the data subject's consent is given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented clearly distinguishable in its appearance from this other matter Provisions on the data subject's consent which are partly in violation of this Regulation are fully void.	2. If the data subject's consent is to be given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.	Bitkom supports the deletion of the red-highlighted EP and Council text.

Article 7 (4), Recital 34 Clear imbalance

A clear imbalance provision as proposed by the Commission in Art. 7 (4) is problematic.

Example: *Company agreements or individual consent by the employee are an important and common instrument to regulate data protection issues between companies and their employees.*

Commission Version Article 7 (4)	EP Version Article 7 (4)	Council Version Article 7 (4)	Bitkom
4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.	1. Consent shall be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected.	**Deleted**	Bitkom supports the deletion of the Commission's proposal regarding the "significant imbalance ".

	The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1), point (b).		Bitkom supports the deletion of the EP - proposal as it is a strong intervention in the freedom of contract. Should this section be maintained, following additions (adopted from §28 (3b) of the German Data Protection Act) should be made: *"The controller may not make the conclusion of a contract dependent on the data subject's consent if access to equivalent contractual benefits is impossible or unreasonable without providing consent. Consent provided under such circumstances shall be invalid."*

Commission Version Recital 34	**EP Version Recital 34**	**Council Version Recital 34**	**Bitkom**
Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This ~~is~~ might be especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.	**Deleted**	34) In order to safeguard that consent has been freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case, where there is a clear imbalance between the data subject and the controller and this imbalance makes it unlikely that the consent was given freely in all circumstance of that specific situation. Consent is presumed not to be freely given, if it does not allow separate consent to be given to different data processing operations despite it is appropriate in the individual case, or if the performance of a contract is made dependent on the consent despite this is not necessary for such performance and the data subject cannot reasonably obtain equivalent services from another source without consent	This Recital should either be deleted altogether like proposed by the EP or the COM`s version of the Recital with the marked slight change in wording should be supported. This wording would make it clear that consent is only obtainable within an employer-employee relation if the imbalance of the relationship does not affect the free decision of the employee. The Council's version is too wide and would cause considerable legal uncertainty in practice.

Article 6 (1) c) and Recital 36 Processing for compliance with a legal obligation

EP Version Recital 36	Council Version Recital 36	Bitkom
Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. This should include also collective agreements that could be recognised under national law as having general validity. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association.	Where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a basis in Union law or in the national law of a Member State It should be also for Union or national law to determine the purpose of processing. ~~Furthermore, this basis could specify the general conditions of the Regulation governing the lawfulness of data processing, determine specifications for determining the controller, the type of data which are subject to the processing, the data subjects concerned, the entities to which the data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing.~~ ~~It should also be for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or by private law such as a professional association, where grounds of public interest so justify including for health purposes, such as public health and social protection and the management of health care services~~	The mention of collective agreements in the EP text is important for the handling of employee data and should be supported and maintained in this Recital. The additional passages of the Council should be deleted as they increase the risk of ending up with different national standards instead of a uniform data protection regime.

Legitimate interest clause and Pseudonymization

Article 6 (1) f), Recital 38 – Legitimate interest of third parties & reasonable expectations

The necessary data processing procedures in a business environment must be simple to implement - i.e. based on the balancing of interest (also in favour of third parties). Circumstances under which permission are granted narrower and less flexible hinder acknowledged and necessary economic processes and can become an obstacle to data processing procedures that become necessary in the future. Bitkom welcomes the reintegration of third parties in Art. 6 (1) (f) GDPR.

Example – Third parties: *Credit agencies and industry warning systems that are partly already legally required to prevent money laundering or fraud 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).*

Example: *Without credit ratings "purchase on account" would not be an option e.g. for online mail order companies because the risk of loss would be too high. Many customers prefer to use this payment method – in particular if they buy at mail order companies they are not yet familiar with. If there were no longer possibilities of uncomplicated credit rating before entering a contract, this would be inconvenient for customers and would to significant downturns in turnover for the companies.*

The concept of "reasonable expectations" leads to big legal uncertainty around Article 6 (1) (f) by introducing enormous subjectivity into an assessment of legitimate interest over and above the existing balancing of interests test. Thereby, it renders the use of the legal basis difficult for the controller and unpredictable in general. Since legitimate interest is a general purpose legal basis, not linked to any specific context, it is not possible to predict with any degree of certainty what an average consumer or a potentially very broad group of data subjects might reasonably expect. In order to determine such expectations a controller had to theoretically create different profiles for all data subject in order to meet their expectations – the reasonable expectation of 80 year old person will differ from a 25 year-old digital native.

Example- reasonable expectations: *Transfers of data processing (processing on behalf) by a company to a third country are generally based on the "legitimate interest of a controller". With the proposed test of the EP, the question arises whether a data subject could have "reasonably expected" at the time of the contract conclusion that e.g. his or her electricity provider would outsource some data processing operations (like billing e.g.) to a foreign country. If not, such outsourcing would not be possible anymore. Furthermore, would the customer "reasonably expect" that his data for e.g. his oil consumption could/will processed by a Big Data analysis one day? Probably not at the time of contract conclusion.*

Example: Users are often unlikely to think about and understand in detail what is required to conduct a certain business. *Customers, for instance, would often not expect that their data are used for a company's analysis (in the context of Compliance) to fight against corruption.*

EP Version Article 6 (1) (f)	Council Version Article 6 (1) (f)	Bitkom
Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: f) processing is necessary for the purposes of the legitimate interests pursued by the controller or, in case of disclosure, by the third party to whom the data is disclosed, and which meet the reasonable expectations of the data subject based on his or her relationship with the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. This shall not apply to processing carried out by public authorities in the performance of their tasks.	Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: f) processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	Bitkom welcomes the reintegration of "third parties" which were missing in the Commission's text. Bitkom believes that references to the user's reasonable expectations should not be made in this context and supports the Council text in maintaining the status quo.

EP Version Recital 38	Council Version Recital 38	Bitkom
38) The legitimate interests of a the controller, or in case of disclosure, of the third party to whom the data are disclosed, may provide a legal basis for processing, provided that they meet the reasonable expectations of the data subject based on his or her relationship with the controller and that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection.	38) The legitimate interests of a controller including of a controller to which the data may be disclosed or of a third party may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding Legitimate interest could exist for example when there is a relevant and appropriate connection between the data subject and the controller in situations such as the data subject being a client or in the service of the controller26. (…) At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can expect at the time and in the context of the collection of the data that processing for this purpose may take place. In particular where such assessment must take into account whether the data subject is a child, given that children deserve specific protection. The data subject should have the right to object to the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests.	Bitkom recommends the deletion of the reference on the "reasonable expectations at the time of the collection " in this and other Recitals in the EP- and Council text.

Provided that the interests or the fundamental rights and freedoms		See comments in Section below.

Article 6 (3) – Harmonization

EP Version Article 6 (3)	Council Version Article 6 (3)	Bitkom
a) Union law, or b) the law of the Member State to which the controller is subject The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. Within the limits of this Regulation, the law of the Member State may provide details of the lawfulness of processing, particularly as regards data controllers, the purpose of processing and purpose limitation, the nature of the data and the data subjects, processing measures and procedures, recipients, and the duration of storage.	c) Union law, or d) the law of the Member State to which the controller is subject The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia the general conditions governing the lawfulness of data processing by the controller, the type of data which are subject to the processing, the data subjects concerned; the entities to, and the purposes for which the data may be disclosed; the purpose limitation; storage periods and processing operations and processing procedures, including measures to ensure lawful and fair processing, including for other specific processing situations as provided for in Chapter IX.	Further specifications to such an extent should be avoided as they run counter to the intended goal of harmonization.

Other example:

EP Version	Council Version Recital 35a	Bitkom
	35a) This Regulation provides for general rules on data protection and that in specific cases Member States are also empowered to lay down national rules on data protection. The Regulation does therefore not exclude Member State law that defines the circumstances of specific processing situations, including determining more precisely the conditions under which processing of personal data is lawful. National law may also provide for special processing conditions for specific sectors and for the processing of special categories of data	This escape clause should be deleted as it is contrary to the Regulation´s goal of reaching a consistent data protection regime throughout the EU.

Defining Anonymization and Pseudonymisation – Art. 4 and Recitals

Although Bitkom appreciates the EP’s and Council’s attempts to provide greater legal certainty around the concept of de-identified data, there are only alleviations for the processing of anonymous data, which falls outside the scope of the GDPR, not the processing of pseudonymous data.

According to the German data protection authorities and the Article 29 Working Group’[1] only data that has been de-personalized in a way that no one can link it to the data subject anymore or only with disproportionate efforts of time or cost can be considered as anonymized data. In other words, anonymization in principle has to be irreversible. Nevertheless, the line between anonymised and pseudonymised data cannot always be drawn easily.

According to this interpretation, most identifiers such as IP- and MAC-addresses would in many cases not be qualified as anonymised data since there is usually one provider or company able to link the identifier to a person or at least a small circle of persons. After many discussions in Brussels it seems to us that the line between pseudonymous and anonymous data on the basis of the Directive and the upcoming Regulation is not drawn in the same way in all member states. Named identifiers appear to be considered anonymized data in some countries, and identifiable data in others. If it is intended to generally look at these categories of data as personal data, so that they fall under the scope of the Regulation, it is necessary to create some privileging rules in order to allow usage as it is common today, for example, for advertising on the internet or the functioning of many connected devices.

Pseudonymous data plays an important role in times of Big Data, Internet of Things, E-health, E-energy and other services, which require the processing of huge amounts of data. By now, the GDPR lacks however clear incentives. The objective to enable the processing of data for new insights and the development of innovative business models while also keeping up a level of data protection for the data subject can be reached with a new legal basis in for the usage of pseudonymous data in combination with an opt-out approach.

Article 4 and Recital 23

EP Version Recital 23	Council Version Recital 23	Bitkom
(23) The principles of data protection should apply to any information concerning an identified or identifiable natural person.	(23) The principles of data protection should apply to any information concerning an identified or identifiable ***natural*** person.	
To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly.	Data including pseudonymised data, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person.	
	To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual directly or indirectly.	This passage must be deleted in order to be in conformity with Art.4 GDPR. Both, EP and Council have deleted such reference in the definition of personal data; therefore, it needs to be deleted in the Recital too.

[1] Working Paper 136 from 2007.

To ascertain whether means are reasonably likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.	To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.	Bitkom believes that this is an important clarification. The simple fact, that certain information theoretically allows the determination of a certain person, should not be sufficient to qualify that information automatically as personal data. Instead, it is crucial by what means, effort and time the individual can be determined.

Article 6 (1) g) - new proposal

Pseudonymous data processing should be deemed lawful for reasons of advertising, market research or to design media services in a needs-based manner (i.e. user interfaces, websites etc.), as long as the profile data is stored separately from the individual data and the pseudonymous profiles cannot be linked to an identifiable natural person subsequently. Furthermore, the data subject needs to get the possibility to opt-out.

Bitkom suggestion:

Article 6 (1) (g) *The processing is limited to pseudonymous data from one or more data sources collected for legitimate purposes of the controller and the data subject is adequately protected. Adequate protection is given if the data has been collected legitimately and the pseudonymization was done in a way that no information can be linked to a certain data subject by a third person and if the data subject is informed in an adequate manner and has the right to object as laid down in Article 19. The pseudonymous data and results of the processing may not be linked with known data of the data subject without his/her prior consent. The results of a combination of data may not cause the identification of the data subject.*

Article 6 (1) h) – new proposal

It further proves difficult, in practice, that there is no clear regulation of data temporary storage for the purpose of anonymization.

Example: *Data that is legitimately collected for one purpose is often further processed and used in anonymized form for another purpose. In order to anonymize the data, it needs to be stored temporarily. Pseudonymous data from different sources are often used to compile anonymized data sets. For such further processing the data needs to be stored temporarily.*

Bitkom suggestion:

Article 6 (1) (h) *The processing serves the anonymization of legitimately collected personal data.*

Recitals 38 and 58a - Pseudonymisation

Recitals alone, referring to “pseudonymous data”, are not sufficient to incentivize such data-friendly processing. However, if integration in the text proves difficult, a corresponding Recital with the content above in context of Article 6 (f) could be drafted.

Should the current Recitals be maintained, even though we do not believe that they provide an adequate solution, we would recommend modifying them. There should be a refutable presumption that when processing pseudonymous data the subject’s interests and fundamental rights and freedoms are not undermined, and his/her interests in not having the data processed do not override the controller’s:

EP Version Recital 38	**Council Version Recital 38**	**Bitkom**
38) The legitimate interests of a the controller, or in case of disclosure …… … Provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, processing limited to pseudonymous data should be presumed to meet the reasonable expectations of the data subject based on his or her relationship with the controller. The data subject should have the right to object the processing, free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks.	(38) …… The legitimate interests of a the controller, or in case of disclosure …… see section above	See comments on reasonable expectation test in section above. **Bitkom suggestion for Recital 38**: *Processing limited to pseudonymous data should be presumed not to trigger privacy concerns that override the interests of the data controller, as long as these are legitimate.*

EP Version Recital 58 a)	**Council Version 58 a)**	**Bitkom**
(58a) Profiling based solely on the processing of pseudonymous data should be presumed not to significantly affect the interests, rights or freedoms of the data subject. Where profiling, whether based on a single source of	(58a) The creation and the use of a profile, i.e. a set of data characterising a category of individuals that is e applied or intended to be applied to a natural person as such is subject to the (general) rules of this Regulation governing processing of	**Bitkom suggestion for Recital 58a** *58a) Profiling based solely on the processing of pseudonymous data should be presumed not to trigger privacy concerns.*

pseudonymous data or on the aggregation of pseudonymous data from different sources, permits the controller to attribute pseudonymous data to a specific data subject, the processed data should no longer be considered to be pseudonymous.	personal data (legal grounds of processing, data protection principles etc.) with specific safeguards (for instance the obligation to conduct an impact assessment in some cases or provisions concerning specific information to be provided to the concerned individual). The European Data Protection Board should have the possibility to issue guidance in this context.	

Article 6(4) and Recitals - Further processing

Such legal basis is essential for many current and future business models. Therefore, German data protection law already allows for further processing in the legitimate interest of the controller.[2]

Examples:
In general, Article 6 (4) plays a significant role for online companies to further develop their services or find completely new business models.

Development of innovative online businesses: *Website providers would be constrained, in how they evaluate the performance of their website if they are not allowed to analyze such data anymore (e.g. to analyze how popular different areas of the websites are or how user-friendly a tool). Out of this data analysis improved or new services can be developed.*

Advertising of online services: *Improved or new services could be offered to those customers, who have previously shown an interest in similar products. Such tailor-made online advertising is crucial for Internet offers and especially for start-up companies to establish themselves on the market. If such a possibility of funding through advertising is prevented innovative business models on the Internet would be obstructed in all conceivable spheres.*

Big Data: *New patterns, unknown correlations, market trends, customer trends and other useful information can be only uncovered when different data sets with different purposes can be combined. A strict purpose limitation would hinder Big Data analytics.*

Credit rating agencies and purchase on account: *Most online shops use credit agencies in order to offer payment methods such as "purchase on account" where businesses make advance payments. This prevents them from taking disproportionate risks.*

If a consumer has not paid his bills, the information will be added to an information base of credit agencies. In a second step this information will be provided to any other requesting business. The transfer of information from a company to a credit agency is not covered by the original purpose (contract for purchase). In such a case, further processing for incompatible purposes is based on the legitimate interest of the controller.

Deletion "by the same controller": The addition "by the same controller" specifically causes problems regarding this credit agency example and should be therefore deleted.

EP Version Article 6 (4)	Council Version Article 6 (4)	Bitkom
deleted	4. Where the purpose of further processing is incompatible	If the Council version stays, Bitkom supports the deletion of

[2] In 28 Abs. 2 Nr. 1, 2 BDSG; §28 Abs. 5 S.2 BDSG; §28 Abs.3 BDSG.

	with the one for which the personal data have been collected by the same controller, the further processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1 . Further processing by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party shall be lawful if these interests override the interests of the data subject.	"by the same controller" (see example above) and recognizes the necessity to provide adequate information (transparency) as laid down in Art. 14 GDPR. In case of deletion of Article 6 (4) and a Recital approach is taken (similar to the clarification of Art. 5 (1) (b) regarding further processing of archiving purposes…), there should be a Recital which clarifies that "further processing by legitimate business models (such as debt collection or credit information services) or (see examples above) is ascertained to be compatible". Here, it must be made clear that the list of given examples is not exhaustive. Otherwise, the technological developments will quickly make these specifications outdated.

Article 8 (1) – Processing of personal data of a child

Bitkom generally welcomes the intention of the Article to protect personal data of children. In practice however, it is difficult to determine the age of internet users. Therefore, it should be further specified what can be reasonably expected from a controller and what kind of "reasonable efforts" he has to make in order to determine the age.

EP Version Article 8	Council Version Article 8	Bitkom
1.For the purposes of this Regulation, in relation to the offering of goods or services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or legal guardian. The controller shall make reasonable efforts to verify such consent, taking into consideration available technology without causing otherwise unnecessary processing of personal data. 1a. Information provided to children, parents and legal guardians in order to express consent, including about the controller's collection and use of personal data, should be given in a clear language appropriate to the intended audience. 2.Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or	1. Where Article 6 (1) (a) applies, in relation to the offering of information society services directly to a child, the processing of personal data of a child shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child or is given by the child in circumstances where it is treated as valid by Union or Member State law. 1a) The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology. 2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or	The text should state a specific age as it leads to legal uncertainty and runs counter to harmonization as Member State laws can differ significantly.

effect of a contract in relation to a child. 3.The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices for the methods of verifying consent referred to in paragraph 1, in accordance with Article 66.	effect of a contract in relation to a child. Deleted	

Article 9 - Processing of special categories of data

The Council, similar to Art. 7 and 8 of the current Directive, takes a risk-based approach by distinguishing between „unambiguous“ and „explicit“ consent depending on the vulnerability and sensitivity of personal data. Bitkom supports the Council text.

EP Version Article 9 (1)	Council Version Article 9 (1)	Bitkom
a) the data subject has given consent to the processing of those personal data for one or more specified purposes, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or	2. Paragraph 1 shall apply where the following applies: (a) the data subject has given explicit consent to the processing of those personal data, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or	Bitkom supports the Council text.

Article 10 - Processing not allowing identification

EP Version Article 10 (1)	Council Version Article 10 (1)	Bitkom
1. If the data processed by a controller do not permit the controller or processor to directly or indirectly identify a natural person, or consist only of pseudonymous data, the controller shall not process or acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. 2. Where the data controller is unable to comply with a provision of this Regulation because of paragraph 1, the controller shall not be obliged to comply with that particular provision of this Regulation. Where as a consequence the data controller is unable to comply with a request of the data subject, it shall inform the data subject accordingly	1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain or acquire (…) additional information nor to engage in additional processing in order to identify the data subject for the sole purpose of complying with (…) this Regulation (…)	Processors should be included in the EP version. Otherwise, it is unclear whether they have to acquire additional information, to fulfil their duties with respect to the GDPR.

	2. Where, in such cases the controller is not in a position to identify the data subject, articles 15, 16, 17, 17a, 17b and 18 do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification.	