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.

Inhalt

Risk-based approach 2

Data protection impact assessment and prior authorization 3

Article 33 (1) – Data protection impact assessment.. 3

Article 33 (4) – Data protection impact assessment.. 4

Article 33 (a) Compliance Review.. 4

Data protection Officer 6

Risk-based approach

The Council makes the notification on data protection breaches dependent on the potential risk to the data subject by the present incident, in contrast to the EP approach where every data protection breach, without exception, has to be reported to the data protection authority.

The risk-based approach by the Council is needed, as it has the potential to substantially improve outcomes for data subjects while reducing administrative burdens for companies:

Serious data protection breaches go unnoticed due to the large scale of incidents reported: In theory, the EP text might contribute to a higher level of data protection. In practice, however, the approach could lead to the consequence, that more serious data breaches, which result in a high risk for the rights and freedoms of the individual, are overlooked by both, companies (not being able to manage the high administrative burden to report each and every incident) and DPAs (due to the information flood). Experience in the US concerning such reporting on credit card data has shown that extensive communication on minor incidents is rather counter-productive as people are over-whelmed with information and tend not to take it serious any more. The other argument in favor of a risk-based approach is that DPAs (Art.31) will not have the capacity (due to tight resources) to manage the workload, when every minor incident is reported. Germany has just evaluated its risk based reporting system and the overall finding was that it works well.

In the EDPS-Strategy[1] the European Data Protection Supervisor stressed that he looks for “practical and workable solutions” and that “data protection needs to be more dynamic and less bureaucratic”. Bitkom supports this view and highlights the well-defined, risk-based approach of the Council on data protection with regard to data breaches **in Article 31, 32, 33 GDPR.**

EP Version Article 31	Council Version Article 31	Bitkom
1. In the case of a personal data breach, the controller shall without undue delay notify the personal data breach to the supervisory authority.	1.In the case of a personal data breach which is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, [breach of (...) pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51. The notification to the supervisory authority shall be accompanied by a reasoned	Bitkom supports the risk-based approach of the Council A company needs a bit of time to evaluate the situation as such. We therefore support the Council approach of 72 hours.

[1] The EDPS Strategy 2015-2019 – Leading by Example.

	justification in cases where it is not made within 72 hours	

Article 32 – Communication of personal data breach to the data subject

In practice, it has been often necessary for a company to refer a data protection breach first to the competent Data Protection Authority to coordiante how to proceed in the specific case and which measureas are appropriate to address the certain problem (e.g. how to secure the data). The notification to the data subject has then taken place afterwards.

Bitkom notes that this procedure is well-established in practice and should be remained. The wording of the Council text to inform the data subject of the data protection breach "without undue delay" might, however, question this practice, depending on how the term is interpreted.

EP Version Article 32	Council Version Article 32	Bitkom
1. When the personal data breach is likely to adversely affect the protection of the personal data**,** the or privacy**,** the rights or the legitimate interests of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay	1.When the personal data breach is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of pseudonymity, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall communicate the personal data breach to the data subject without undue delay.	Bitkom supports the risk-based approach of the Council. Please see comments above

Data protection impact assessment and prior authorization

Article 33 (1) – Data protection impact assessment

EP Version Article 33 –	Council Version Article 33	Bitkom
1. Where required pursuant to point (c) of Article 32a(3) the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the rights and freedoms of the data subjects, especially their right to protection of personal data. A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.	1.Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, the controller shall**,** prior to the processing, carry out an assessment of the impact of the envisaged processing	Bitkom supports the risk-based Council approach in Section 1 (see comments above)

	operations on the protection of personal data.	

Article 33 (4) – Data protection impact assessment

The requirement to seek the views of data subjects or representatives like consumer protection organizations is totally disproportionate and should be therefore deleted.

EP Version Article 33	Council Version Article 33	Bitkom
	4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.	Bitkom supports the deletion of the Council text.

Article 33 (a) Compliance Review

Bitkom generally supports compliance reviews especially in light of an adequate and effective risk management approach at a company. From a practical viewpoint, a two-years-period is relatively short, especially for SMEs and start-ups. Independent of what period is stated, a static year-based compliance review does not give an additional benefit where no change in the processing operation has occurred or the circumstances have significantly changed. The effort needed to do such 2-year-review by no means justifies the benefit.

Therefore, Bitkom supports the deletion of reference of time. In case of a compromise, the compliance review must be incident-based.

EP Version Article 33 (a)	Council Version Article 33 III	Bitkom
.At the latest two years after the carrying out of an impact assessment pursuant to Article 33(1), the controller or the processor acting on the controller's behalf shall carry out a compliance review. This compliance review shall demonstrate that the processing of personal data is performed in compliance with the data protection impact assessment 2.The compliance review shall be carried out periodically	8. At the latest two years after the carrying out of an impact assessment, the controller shall carry out a compliance review to assess if the processing of personal data is performed in compliance with the data protection impact assessment. The compliance review shall be carried out periodically at least every two years, or immediately when there is a change in the specific risks presented by the processing operations. → covers Article 33a EP text	Bitkom supports the deletion of "two years". **Compromise suggestion:** The controller shall carry out a compliance review in case of a change of data processing or where the circumstances have significantly changed.

at least once every two years, or immediately when there is a change in the specific risks presented by the processing operations Where the compliance review results show compliance inconsistencies, the compliance review shall include recommendations on how to achieve full compliance.		

Data protection Officer

Bitkom supports the concept of „Data Protection Officer“ (DPO) in companies as the integration of this model has been very successful in Germany and proven that there are benefits for both, the data subject on one hand and companies on the other hand.

Following points should be taken into consideration for an effective integration of DPO in the GDPR:

- **Independency and professional secrecy:** The DPO's strong position and direct line of report to the executive level make him an effective and independent supervision authority within a company. To strengthen the position of the DPO, continuous professional training, independency and professional secrecy should be guaranteed.

  ➔ **The model of independent DPOs with direct line of report to the executive level is well-proven and should be implemented.**

- **Replacing notification and consultation obligations:** The appointment of a DPO should be advantageous for companies –e.g. by replacing notification and consultation obligations as under existing national data protection law. This would give incentives for companies to integrate a DPO and at the same time help to reduce the administrative burden. It would also address the concerns of opponents that an obligatory DPO is not a high burden for SMEs and start-ups.

  ➔ **There need to be incentives for companies to appoint a DPO.**[2]

- **Auditing of BCRS:** A DPO should be generally allowed to audit in the context of BCRs also the respective subsidiaries.

- **Different termination periods:** It should be clearly stated, that a DPO cannot only be an employee of the controller but also be an independent external service provider. Different termination periods for DPO contracts are not in the interest of the data subjects and should be therefore avoided. A longer period for internal DPOs implies the risk of preference for externals as the company does not want to be bound for four years by the same person.

  ➔ **No difference between Internal and External DPOs should be made.**

EP text Article 35 7)	**Council text 35 7)**	**Bitkom**
7. The controller or the processor shall designate a data protection officer for a period of at least ~~two~~ ***four*** *years* ***in case of an employee or two years in case of an external service contractor***.	7. ~~The controller or the processor shall designate a~~ ***During their term of office, the*** data protection officer ~~for a period of at least two years. The data protection officer~~ may***, apart from serious grounds under the law of the Member State concerned which***	Bitkom support the deletion of reference to termination periods

[2] See Art. 18 (2) and Art. 20 (2) of Directive 95 /46; See German Data Protection Act e.g. in §4d (2) BDSG.

The data protection officer may be reappointed for further terms. During ~~their~~ ***his or her*** term of office, the data protection officer may only be dismissed, if ~~the data protection officer~~ ***he or she*** no longer fulfils the conditions required for the performance of ~~their~~ ***his or her*** duties.	***justify the dismissal of an employee or civil servant,*** ~~be reappointed for further terms. During their term of office, the data protection officer may only~~ be dismissed~~,~~ ***only*** if the data protection officer no longer fulfils the conditions required for the performance of ~~their duties~~ ***his or her tasks pursuant to Article 37***.	