bitkom

Position Paper

Bitkom views on Article 29 Working Party draft guidelines on automated individual decision-making including profiling

27/11/2017

Bitkom represents more than 2,500 companies of the digital economy, including 1,700 direct members. Through IT- and communication services only, our members generate a domestic turnover of 190 billion Euros per year, including 50 billion Euros in exports. Members of Bitkom employ more than 2 million people in Germany. Among the members are 1,000 small and medium-sized businesses, over 400 startups and nearly all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the sectors of digital media or are in other ways affiliated to the digital economy. 80 percent of the companies' headquarters are located in Germany with an additional 8 percent each in the EU and the USA, as well as 4 percent in other regions. Bitkom supports the digital transformation of the German economy and advocates a broad participation in the digital progression of society. The aim is to establish Germany as globally leading location of the digital economy.

Federal Association
for Information Technology,
Telecommunications and
New Media

Susanne Dehmel
Managing Director
Law and Security
P +49 30 27576 -223
s.dehmel@bitkom.org

Rebekka Weiß, LL.M.
Data Protection &
Consumer Law
P +49 30 27576 -161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

1. Introduction

Bitkom welcomes the opportunity to comment on the Art. 29 Working Group's (WP29) draft opinion on the **interpretation of automated individual decision-making including profiling** (WP 251). We believe that more cooperation and exchange between data protection authorities and practitioners is needed to translate the legal text of the GDPR into practice and reduce legal uncertainty.

In addition to many other provisions of the GDPR, Article 22 must be implemented until May 2018 not only by the digital economy but also by all other sectors. This should not pose a major challenge to companies as the **provision does not constitute a fundamental change to current data protection law**.[1] Therefore, current legal commentary on Directive 95/46/EC (Directive) as well as jurisprudence (case law), which draw a **clear distinction between 'profiling' on the one hand and 'automated**

[1] This view is shared by many data protection scholars, see for example Roßnagel/Nebel/Richter ZD Jahr 2013 108; Roßnagel VUR Jahr 2015 362.

decision-making' (decisions) on the other hand, can be taken into account as reference points for interpretation.

In contrast, the **WP29 does not follow the current approach and merges these two areas of data processing (profiling) and automated decision-making** in the entire text, starting with the definitions in Chapter II. This blurring of legal requirements of the GDRP leads to great legal uncertainty for companies in different sectors.

The aim of this position paper is to draw attention to the difficulties in interpreting and implementing the law. **Chapter 2** addresses the general concerns of the current WP29 approach, whereas **Chapter 3** deals with specific aspects of the draft opinion and comments on concrete statements of the text based on the structure laid down in the WP29 draft guidelines.

2. General remarks

- **Definition:** 'Profiling' is defined in Art. 4 No. 4 GDPR, whereas the term 'automated decision' in Art. 22 GDPR is not explained in more detail. The legislator presumably assumed that this term was self-explanatory and meant something other than profiling. Profiling and decisions are obviously different things that should not be intertwined. To define the 'automated decision', current commentary on Art. 12/15 of the Directive can be taken into account where it is laid down that there are '**decisions' in the sense of a yes/no logic** as well as **'decisions' which are preceded by profiling.** Conversely, it is also conceivable that there may be a **mere profiling which does not lead to a 'decision'.** The latter occurs in principle with all data traders like in the advertising industry or credit agencies. Yes/no processing is also allowed if it does not lead to a 'decision' (pre-selection). To sum up, **'Profiling' is not congruent with an 'automated decision'. Even at the definition stage, a clear separation is necessary, because otherwise the follow-up questions will also be mixed.**

- **Legal nature of profiling (results):** While a 'decision' has a direct impact on the data subject and should therefore be specifically regulated, 'profiling' represents a data processing result (**output data**). **According to (German) case law, such profiling result should not be qualified as a statement of fact but rather as a value judgment and thus as an expression of opinion**.[2] This type of opinion-forming is also allowed as long as it is based on sufficient (many) true (individual) facts.

- **Admissibility requirements:** The legal bases of data processing are exhaustively defined in Art. 6 GDPR. However, with regard to profiling the question often arises whether special requirements apply. This is denied by the currently available legal commentary (at least in Germany).[3] **It is widely accepted by scholars, that the legal basis of profiling (or data processing which leads to profiling) can be derived from Art. 6 (1)(f) GDPR. In this respect, no special provisions or restrictions apply to profiling**.

  Basically, it needs to be **considered first whether the processing of input data** is allowed under the GDPR. If this is the case, the profiling result obtained from such data should also be valid. **According to (German) case**

[2] German Supreme Court (Bundesgerichtshof), BGH 22.02.2011 – VI ZR 120/10.
[3] See e.g. Beck DatenschutzR/von Lewinski DS-GVO Art. 22 Rn. 1-4; Paal/Pauly, Datenschutz-Grundverordnung DS-GVO Art. 22, Rn. 21-23 etc.

law, it is therefore (only) important whether the processing of individual facts/data is allowed that lead to a 'profiling result.'[4]

Furthermore, there is a provision for 'automated individual decision-making'. First, the question arises as to whether this is a right of the data subject or an absolute (processing) ban to be placed on the admissibility level. **Bitkom supports the first interpretation and considers Art. 22 GDPR as the right, not to be subject to a decision based solely on automated processing** (para. 1) which is subject to certain exceptions (para. 2). Regardless of whether the WP29 follows this view, **only the 'automated decision' is prohibited but not the processing that may have taken place before** even if this includes profiling. Such processing is governed by Art. 6 of the GDPR.

Last but not least, the 'decision-making' needs to **produce either 'legal effects' or 'similarly significant effects' which are significantly more than trivial** and highlight that such level is reserved only for the most impactful automated decision-makings.

- **Data Subject Rights**

Right of access by the data subject: Two dimensions need to be considered:

- **The right to obtain information and access to the personal data** needs to be provided according to Art. 15 GDPR.

- However, in the **case of a profiling (result), this is only relevant if the result has actually been stored and can be qualified as personal data**. However, according to the German Supreme Court, the **profiling result is not a (own) fact and thus personal data, but rather a value judgement or expression of opinion (obtained from data).**

Transparency Obligation

In addition, it should be noted that Art. 15 (1)(h) GDPR specifically refers to 'automated decision-making' in Article 22 GDPR. However, even if Art. 22 GDPR is interpreted in such a way that the information requirement does not only refer to an 'automated decision' but is extended to cover also profiling as such, **the question still remains as to how far the obligation to provide information extends.**

Here, in view of the concept of meaningful information about the 'involved logic' **it should be sufficient to provide information about the underlying procedure,** taking into account that such information should be simple according to Art. 12 GDPR and does not need to include complex explanations. In this context it should be noted that **while every data subject can invoke the right of access to the profiling**

[4] German Supreme Court (Bundesgerichtshof, BGH, 28.01.2014, VI ZR 156/13.

basis (personal data), only supervisory authorities - which are bound to confidentiality – can (have the right and capacity) to examine (the scientific nature of) the procedure.

Attention should be paid in particular to the fact that, according to case law, there is a **predominantly legitimate interest in the secrecy of the formula for calculating a decision**. The contents of such a formula/algorithm that are protected as trade secrets are the calculated variables, such as the statistical values used, the weighting of individual calculation elements in determining the probability value and the formation of possible comparison groups.

To sum up, the right of the data subject to be informed is limited by the requirement to keep the formula/algorithm confidential. **A general balance must be found between the need for transparency and the protection of trade secrets.** For example, the data subject is protected by the disclosure of the personal data included in the calculation, but not by the disclosure of details of the calculation procedure.

Rectification and erasure: If, according to the German Supreme Court, **it is assumed that the profiling result is an expression of opinion, rectification and deletion cannot be applied**, see also Art. 17 (3) GDPR. However, the data subject is sufficiently protected by Art. 16 and 17 GDPR as he or she has influence on the personal data (data basis) underlying the expression of opinion.

Final conclusions: For the draft guidelines of WP29 this means that:

1. **'Profiling'** and **'automated decision'** are different things that should not be intertwined. **Even at the definition stage, there should be a clear separation because otherwise the follow-up questions will also be mixed.**

2. It is generally necessary to differentiate between different cases, such as **profiling** which does not lead to a decision, **automated decisions** and **automated decisions preceded by profiling** (subgroup). **Blurring the legal requirements of different cases creates legal uncertainty.**

3. **The admissibility of profiling** (or data processing leading to profiling) is **derived from Art. 6 GDPR. There are no special requirements/restrictions for profiling.**

4. **Art. 22 GDPR,** like all other provisions in Chapter III, **needs to be qualified as a data subject right.** This 'right, not to be subject to a decision based solely on automated processing' (para. 1), is subject to certain exceptions (para. 2).

5. Art. 22 GDPR focuses on **'automated individual decisions'**, including those based on profiling (subgroup), and chooses **not the individual processing step** as reference point, **but the 'decision' based on it.**

6. For an automated decision-making to produce '**similarly significant effects' it must rise to the same level as producing a 'legal effect' which is a high bar**. Reaching such a level is reserved for only the most impactful automated-decision makings.

7. **A distinction must be generally drawn between input data**/raw data/data basis **and output data**, e.g. the conclusions that the company draws on the basis of the raw data. The latter cannot only be viewed from a data protection perspective. **Other fundamental rights need also be taken into account.**

8. As emphasized by courts, there is a **predominantly legitimate interest in the secrecy of the formula for calculating a decision**. Therefore, **the need for transparency and the protection of trade secrets must be generally balanced.**

9. In line with jurisprudence, **processing of the individual facts/data (input data)**, which leads to a profiling result, **should be in line with general requirements of the GDPR**. However, a profiling result is not a (own) fact and thus cannot necessarily be qualified as personal data, but rather a value judgement (obtained from data) or expression of opinion (protected as fundamental right), which is obtained on the basis of reliable facts.

10. The **data subject shall have the possibility to verify the accuracy of the data basis and, in case of incorrectness, to demand its correction**. If, however, it is assumed that the **profiling result** is an expression of opinion, **further procedural rights such as rectification and erasure** cannot apply.

2.2 Comments on the W29 text

In the following, statements of the WP29 draft are commented on. The text quoted from the draft guidelines is highlighted in italics.

I. Introduction

II. Definitions

I. Definitions: 'The GDPR does not focus on the decisions made as a result of automated processing or profiling. It applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals.' p. 6

From Bitkom's perspective, **this interpretation cannot be based on either the wording or the history of the Art. 22** as the **GDPR (like the Directive before) chooses not the individual processing step as reference point for the provision, but the decision based on it**. This results not only from the wording which emphasizes a subsequent decisions ('based on') but also stems from the history of the GDPR. Originally, the European Parliament had proposed a wide 'profiling' provision, according to which each data subject 'shall have the right to object to profiling in accordance with Article

19.'[5] However, this approach was rejected in favour of a wording which focused (already in the heading of the Article) on 'automated decision-making' and not 'profiling'.

III. Specific Provisions on Automated Decision-Making as Defined in Article 22 GDPR

A. Based Solely on Automated Processing

B. Legal or Similarly Significant Effects

- *'Recital 71 GDPR provides the following typical examples: 'automatic refusal of an online credit application' or 'e-recruiting practices without any human intervention'. These suggest that it is difficult to be precise about what would be considered sufficiently significant to meet the threshold. For example, based on the recital each of the following credit decisions fall under Article 22, but with very different degrees of impact on the individuals concerned: [...] - purchasing a kitchen appliance or a television set on credit; - obtaining a mortgage to buy a first home.' p. 10*

  The abovementioned examples are provided in the draft guidelines as examples of automated decisions with a 'similarly significant' effect. However, they clearly have a legal effect and citing them as examples of 'similarly significant' (i.e. non-legal) effects leads to legal uncertainty. **From Bitkom's perspective, there is a need to provide further and more distinctive examples.**

- *'[...] Advertising or marketing practice do not fall under Article 22 [...]' p. 11*
- *'Processing that might have little impact on individuals generally may in fact have a significant effect on certain groups of society, such as minority groups or vulnerable adults. For example, someone in financial difficulties who is regularly shown adverts for online gambling may sign up for these offers and potentially incur further debt.' p. 11*

  Profiling for advertising purposes should, according to the WP29, generally not fall under the scope of Art. 22 GDPR. **Bitkom shares this view** as direct marketing and advertising are generally considered to be activities in the legitimate interest of the controller in accordance with Art. 6 (1)(f) GDPR.

  However, it is further stated that under certain circumstances the scope extends to advertising profiling and an example is given on advertisements for online gambling aimed at an over-indebted adult. **From Bitkom's perspective, it is unclear how this exception is to be understood:**

  - Does the data controller/processor – when using profiling - have to be aware of the fact that the data set belongs to a 'vulnerable adult' and that the corresponding advertising is then sent to or shown in context where it must be assumed that this group is addressed directly? (e. g. advertising alcohol on a website of the

[5] *See* Bitkom Comments on Chapter III - Rights of data subject, https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/Trilogverhandlungen/2015-12-10-Bitkom-Comments-on-Chapter-IV-PART-1-Controller-and-Processor-FIN.pdf.

anonymous alcoholics).

- Or is it already sufficient if this advertising can be read objectively by such an adult?

The latter would be highly problematic because this information on vulnerable adults is not available in the context of advertising profiling. Usually, advertisers do not know whether the recipient of their advertising campaign is over-indebted or an alcoholic (without collecting additional information on the user).

A similar question arises with regard to the comments on **advertising to children** (p. 26). In this context, it is also not clear to which age group the WP29 refers to when stating that '*children represent a more vulnerable group of society, organizations should, in general refrain from profiling them for marketing purposes.*' It should be noted that the study cited by the WP29 on marketing refers only to 6-12 year-olds and not to teenagers.

- *'Automated decision-making that results in differential pricing could also have a significant effect, if, for example, prohibitively high prices effectively bar someone from certain goods and services.' p. 11*

Many follow-up questions arise regarding differential pricing:
- How are 'prohibitively high prices' defined given that each financial situation is unique?
- Are websites that offer flights and hotels able to provide different pricing options based on cookies and/or a data subject's behaviour on the website?
- Would certain things like selective discounts meet the 'differential pricing' standard?

- *'However, it is possible that it may do, depending upon the particular characteristics of the case, including: the expectations and wishes of the individuals concerned.' p. 11*

Such a test, which is based on **subjective criteria** ('wishes of the data subject'), **leads to a high degree of legal uncertainty in practice** and is impossible to predict. The focus should lie on aspects which can generally be predicted.

- '*Similarly significant effects may be positive or negative.' p. 11*

'Similarly significant effects' should be interpreted to only cover automated decisions with a negative effect. Where automated decisions have a positive effect (e.g. health and social benefits), they should not be considered to have a 'similarly significant effect' and should therefore not be considered as a 'prohibited' automated decision under Art. 22 GDPR. This has the advantage of ensuring that individuals get the benefits from such automated decisions even if they have forgotten to submit a certain consent form. At a minimum, automated decisions with a merely positive effect should be subject to a less strict regime in terms of transparency requirements, in particular, in relation to the requirement to provide meaningful information about the logic involved, the significance and the envisaged consequences of the automated decisions.

C. Exceptions from Prohibition

- *'Article 22(1) sets out a general prohibition on solely automated individual decision with a significant effect, as described above.' p. 12*

  Bitkom does not support the interpretation that Art. 22 (1) GDPR sets out a general prohibition. In practice, such a general prohibition would also restrict the use of technology to the benefit of individuals. Rather than a general prohibition, **Art. 22 (1) provides data subjects with a right, 'not to be subject' to automated decisions**. This is a right that requires a positive action by the data subject, who must inform the data controller (upon receiving the required transparency information on the automated decision) that he/she does not wish to be subject to the automated decision. This interpretation is in line with the other rights under the GDPR, which also require a positive action (e.g. the right to access, rectification, or erasure).

D. Rights of the data subject

Right not to be subject to a decision

- *'Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a thorough assessment of all relevant data [...].'p.16*

  It should be clarified that the nature and scope of human intervention in a given automated-decision-making is contextual and can include a range of measures. The ultimate goal of human intervention should be to ensure a correct automated processing and fair decision.

IV. General Provisions on Profiling and Automated Decision-Making

A. Data Protection Principles

1. **Article 5 (1) (a) – Lawful, fair and transparent**
2. **Article 5 (1) (b) – Further processing and purpose limitation**
3. **Article 5 (1) (c) – Data minimisation**
4. **Article 5 (1) (a) – Accuracy**

- *'Controllers should consider accuracy at all stages of the profiling process [...]' p. 19.*

The difference between input data/raw data/data base (input data) and output data should be also considered in this context.

Example Artificial Intelligence: Art. 5 (1)(d) GDPR stipulates that personal data must be accurate and, where necessary, kept up to date. The input data of algorithms must therefore be correct, complete and up-to-date. This is already considered in data quality management and in the interest of good analysis results. In terms of output data, however, the principle leads to considerable uncertainty. Only facts are accessible to proof and can therefore be

correct or incorrect. Often, however, the output data will be forecasts of the future or opinions to which the principle of data correctness is not likely to apply.[6]

5. Article 5 (1) (e) – Storage limitation

'Machine-learning algorithms are designed to process large volumes of information and build correlations. Storing collected personal data for lengthy periods of time means that organisations will be able to build up very comprehensive, intimate profiles of individuals, since there will be more data for the algorithm to learn. Even if collection of the information fulfils the requirements of purpose specification and relevance, storing it for a long time may conflict with the proportionality consideration, i.e. the method may be too intrusive in terms of the individual's right to privacy. Keeping personal data for too long also increases the risk of inaccuracies.' pp. 19-20.

The interpretation provided is not helpful in relation to profiling and automated decision-making.

Firstly, Art. 5 (1)(e) GDPR provides for **personal data to be retained for as long as '*necessary for the purposes for which the personal data are processed*'. This should not be different for profiling.**

In addition, **retaining personal data for longer periods actually increases the accuracy of the profiling** undertaken with such data. The technology behind profiling is such that the more data is taken into account by the profiling algorithm, the more accurate the profiling will be. Storing the data for longer periods will therefore be advantageous for data subjects, as it ensures that any profiling relating to such data subjects is as accurate as possible.

Secondly, the words 'lengthy periods' and 'too long' are vague terms. It is unclear who will determine what a 'lengthy period' and 'too long' means. This could have the consequence that, even if data is still necessary for automated decisions, a data controller could deem that it has retained the data 'too long' and therefore delete it. Such decision would have two consequences:

- (i) the profiling would become less accurate (as explained above) and
- (ii) data subjects would suddenly be confronted with their data (e.g. their photos, website orders, transaction history) no longer being recoverable**.**

Bitkom therefore suggest deleting these vague terms 'lengthy periods' and 'too long' and simply referring to the above-mentioned principle of Article 5 (1)(e) GDPR.

[6] *see* Bitkom Guidelines on Artificial Intelligence, "Leitfaden Entscheidungsunterstützung mit Künstlicher Intelligenz" p. 136. A short version of the paper is also available in English https://www.bitkom.org/Bitkom/Publikationen/Entscheidungsunterstuetzung-mit-Kuenstlicher-Intelligenz.html.

E. Rights of the data subject

1. Articles 13 and 14 – Right to be informed

'The controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision without necessarily always attempting a complex explanation of the algorithms used or disclosure of the full algorithm. The information provided should, however, be meaningful to the data subject.' p.14

There should be specific clarification in the guidelines that there is no requirement to disclose a full algorithm to a data subject, as it does not constitute a *'simple way to tell the data subject about the rationale or the criteria relied on'*. In addition, any transparency obligation needs to be balanced with the rights of the data controller and third parties. An algorithm can constitute intellectual property and/or confidential information of the data controller or a third party and a disclosure requirement may therefore violate these rights. Any disclosure requirement must only be in specific cases where there is, for example, a requirement by authorities (e.g. in the case of law enforcement or fraud investigation), and not to individual data subjects.

2. Article 15 - Right of access

'The right to obtain details of any personal data used for profiling, including the categories of data used to construct a profile [...] However, only under rare circumstances should these rights outweigh individuals' right of access; controllers should not use this as an excuse to deny access or refuse to provide any information to the data subject' p. 24.

According to the German Supreme Court, the right of access refers to the specific personal data that has been included in the algorithm/formula. **No disclosure must be made as to which data had a concrete influence on the calculation (this would be tantamount to disclosure of the formula/algorithm) and as to the identity of the peer groups and the reasons for which the data subject was assigned to the peer groups.**[7]

Example credit agency: A data subject claimed the right of access under data protection law. She received a data overview from the credit agency which contained, in addition to the stored personal data, general information on the data subject and on the scoring procedure. For data types, the credit agency indicated whether they were used or not. However, the data subject asked for the individual elements that have been included in the calculation of the score (probability value for the future behaviour of groups of people on the basis of a statistical-mathematical analysis method) to be disclosed and information on the comparison groups to be provided. This claim was, however, dismissed by the court.[8]

3. Article 16 – Right to rectification/ Article 17 Right to erasure / Article 18 Right to restriction of processing

'The right to rectification applies to the input applies to the 'input personal data' (the personal data used to create a profile) and to the 'output data' (the profile itself or 'score' assigned to the person, which is personal data relating to the

[7] See also CJEU, EuZW 2009, 546 Rn. 49 f. –Rijkeboer.
[8] German Supreme Court (Bundesgerichtshof) BGH, 28.01.2014, VI ZR 156/13.

person concerned)' p. 24. 'Similarly the right to erasure will apply to both the input and the output data' p. 25.

Rectification can generally not apply with regard to a probability forecast. This would also jeopardise the fundamental right of expression (see also case law on review platforms). Rectification can only take place if the data on which it is based are incorrect. Erasure is also not applicable if the profile result cannot longer be qualified as personal data.

IV. Children and Profiling

See remarks on page 6.