55.

bitkom

Position Paper

Bitkom views on Article 29 Working Party draft Guidelines on the right to data portability (WP 242)

31/01/2017

Bitkom represents more than 2,400 companies in the digital sector, including 1,600 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.

Federal Association
for Information Technology,
Telecommunications and
New Media

Susanne Dehmel
Member of the Executive Board for
Security and Trust
P +49 30 27576 -223
s.dehmel@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Thorsten Dirks

CEO
Dr. Bernhard Rohleder

1 Introduction

Bitkom welcomes the opportunity to comment on the Art. 29 Working Group's draft opinion on the interpretation of the new duty of data portability. 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.

In our working group on data protection we gather more than 600 data protection professionals, of which most are practicing data protection officers, who are currently commonly working on the interpretation and application of the GDPR. Bitkom has dedicated considerable efforts both into the process accompanying the making of the GDPR as well as now the implementation phase. In this process we have identified a number of concrete, practical issues which we would be happy to highlight and thereby contribute to the work of the WP29, especially as neither Bitkom nor its members were given the opportunity to take part in the GDPR FabLab workshop in July 2016.

bitkom

2 General remarks on the views on Article 29 Working Party draft guidelines

While Bitkom welcomes guidance on the application of the GDPR, we are concerned that the draft opinion risks significantly expanding the scope the regulation. It appears to deviate from or go beyond the results of the extensive process and political discussion around the creation of the GDPR. In consequence, it creates new levels of legal uncertainty for companies and data subjects alike. Furthermore, the Opinion is silent on many legal as well as practical questions which have been raised by data academics and practitioners. Due to the short deadline set by the WP29, only some of these aspects can be highlighted in this paper.

2.1 Interpretation considerations

- **The wording of Art. 20 should be the basis for interpretation** of the right to data portability. Any further requirements like e.g. "that all customers must be informed at the time of account closure about the right to data portability" (p. 11) are not grounded in Art. 20. It is therefore doubtful whether the WP29 can introduce/expect companies to comply with new requirements.

- **Systematically,** the GDPR introduced the right to data portability in addition to already existing data subject rights such as the right to information and access of personal data, the right to rectification and erasure. It thus should be **interpreted in the context of and distinguished from these other rights**.

- In this context, the **legislator has consciously limited the personal data affected by the right to data portability to data "provided to a controller" by the data subject**. This wording was deliberately chosen over "processed" personal data as laid down in other data subject rights. This approach avoids conflicts regarding the different rights of data controllers, data subjects and third parties while also creating an easy to exercise right for the data subject. Any further going interpretation contradicts this limitation.

- Furthermore, Art. 20 must be also **interpreted in light of the purpose and goal of the legal provision.** As stated in the EU Commission's *detailed explanation of the proposal* the main purpose and goal of the right is **"to transfer data from one electronic processing system to and into another**, without being prevented from doing so by the controller." Further, it is stated that "as a precondition and in order to **further improve access of individuals to their personal data,** it provides the right to obtain from the controller those data in a structured and commonly used format" (p. 9, Com (2012) 11 final from 25.1.2012). Also in Recital 68 it is only stated that the right should "**strengthen the [data subjects] control over his or her own data**".

  The WP29 should in its Opinion take into account more the purpose and goal of the provision, namely to transfer the person's data from an automated data processing system to another system. In light of the main purpose, the emphasis should be on **data which is closely related to the service** (from controller A) and is necessary to make the new service (from controller B) useful. All other data is addressed and covered by the right of information and the right to access data in the GDPR. This idea is supported by the examples which the WP29 has given in its Opinion such as the playlist of a streaming service or the performance

record of a fitness app which are both closely linked to the service. What data is closely related to the service can only be identified on a case-by-case basis. Such narrow interpretation would also prevent that the rights stemming from intellectual property law and trade secrets and the rights and freedoms of third parties are not affected.

We acknowledge that the GDPR shall also enable the free flow of data, however, this shall be achieved as stated in Recital 13 through "legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises and to provide natural persons in all MS with the same level of legally enforceable rights [...]. " In contrast to this, the WP29 is referring to many other external considerations e.g. "foster competition between controllers" and "foster the development of new services"(p. 3) which are not at the essence of data protection and also not mentioned in Recital 68 to interpret Art. 20.

- Furthermore, many other aspects need to be considered when interpreting the law. Not only that the right "**shall not adversely affect the rights and freedoms of others**" (Art. 20 (4)) or "not apply to processing necessary for the performance of a task carried out in the public interest" (Art. 20 (3)) but also other **possibly conflicting laws** like special provisions under EU as well as national law (e.g. in the telecommunications sector) need to be taken into account.

- Finally, the **proportionality principle** should be taken into account by the WP29. The interpretation of Art.20 GDPR should be limited to what is necessary to achieve the objective as stated above.

2.2 Practical considerations

- We welcome that the WP29 points to the development of common standards and interoperable systems creating easy ways to enforce the right to data portability. **However, it must be clear that this cannot mean an establishment of open API layers until the GDPR will enter into force**. The development of technical standards is a challenging process, requiring considerable time and effort from many parties involved, including supervisory authorities and public entities.

- Furthermore, it should be noted that "**APIs" will not be a desirable or feasible option in all sectors of the economy.** In general, standards are developed within specific sectors like banking, telecommunications, healthcare, transport or the retail industries. The main benefit of the data portability right lies not only in the simple transfer of data but also in enabling the data subject to actually use the data in a new service. Therefore, purpose and goal of Art. 20 should be taken into account in this context as well as the proportionality principle. **The development of cross-sectoral standards would contradict the proportionality principle as it represents both an excessive burden for companies and in most cases, it is not technically feasible.** It also not necessary to achieve the main purpose of Art. 20 as stated above. Finally, there are also less restrictive and more suitable means to "foster the development of new services". Therefore, the WP29 should encourage standards and formats enabling the data subject to reuse any data provided and thus facilitating switching between service providers within a sector.

3. Main elements of data portability in Art. 20 GDPR

1. Personal data concerning the data subject pursuant to Art. 4 GDPR
2. Data must be "provided" by the data subject
3. Processing is based on consent or contract pursuant to Art. 6 (1)(b)
4. Processing is carried out by automated means

3.1 Personal data

It appears clear that the provision applies only to "personal data" pursuant to Art. 4 No. 1 GDPR and to "natural persons". According to WP29, the requirement "personal data concerning the data subject" is not to be interpreted too narrowly.

As an example, the Opinion mentions that telephone records may include details of third parties involved in incoming and outgoing calls. Although records contain personal data of multiple people, subscribers should be able to have these records provided to them in response to data portability requests. However, where such records are then transmitted to a new data controller, this new data controller should not process them for any purpose which would adversely affect the rights and freedoms of other third-parties.

This example is very difficult as it refers to the telecommunication sector which is subject to additional legal requirements. Furthermore, a data controller cannot easily disclose information which would infringe the confidentiality of third parties. In general, Art. 20 can only be interpreted to the extent that problems with the rights of freedoms of third parties are avoided. In this context, it should be noted that the data subject should not be brought into the difficult situation where it might be liable for the infringement of rights and freedoms of others e.g. under civil law claims. It would be generally helpful if the Art. 29 Group could provide more examples here.

3.2 Data "provided to a controller"

The interpretation of personal data that a data subject **"has provided"** to a controller poses even more challenges as the GDPR does not legally define what "provided to a controller" actually means.

- The WP29 first distinguishes between **"knowingly and actively provided data"** e.g. account data (such as mailing address, user name, age, etc.) entered by online forms and **"observed data"** that are "provided" by the data subject by virtue of using a service or the device (e.g. raw data created by a smart meter, raw data such as the heartbeat tracked by a fitness or health tracker, a person's search history, traffic and location data). The WP29 appears to consider **both newly established categories as data which has been "provided" by the data subject.**

- "Not provided" by the data subject is, according to the interpretation of the WP29, **"inferred or derived data"** which has been created by a data controller on the basis of the data "provided" by the data subject

e.g. a credit score, the result of a health check or the user profile which has been created by e.g. the raw data of a smart meter. **This data category should therefore be outside the scope.**

Question: In the case of the data resulting from the use of a service or product ("observed data"), the question arises whether this refers only to the data which is also relevant to the functionality of the service and therefore also plays a role for a possible change of provider or whether, for example, also by-products are included (such as log-files and metadata).

Bitkom considerations:

From an interpretation point of view (see also 2.1): If one considers that the legislator has deliberately chosen the wording "provided" over "processed" as stated above, it should be sufficient to only consider the data that the data subject controls and accesses on its own (e.g. photos, emails during the performance of the contract) . Thus, this would exclude usage data necessary data for the conclusion of the contract. In particular, the controller should not be obliged to provide any data which has been generated automatically by the service while the data subject is using the service (logfiles, traffic and location data).

From a technical point of view: most service providers do not have a separate data base containing only the raw data that can easily be separated from the algorithms to create profiles for customer analytics. Transferring this data to another service provider would in almost all cases give detailed background information about the technical setup of the original controller and the algorithms used. This would risk revealing core technical and business information, which in most cases is protected by intellectual property rights and trade secrets. Since the "rights and freedoms of others" as laid down in Art. 20 (4) GDPR are not to be affected, data controllers cannot be obliged to provide such data.

Example: electronic communications data:
Question: Especially for electronic communication data with legal deletion obligations, the right to data portability creates a myriad of legal uncertainties. Traffic and location data **should not** be interpreted as data "provided" by the data subject for the following reasons:

Purpose and goal of Art. 20 GDPR (see also 2.1): As stated above, Art. 20 GDPR must be interpreted in light of the purpose and goal of the provision. In order to enable the data subject to move from one service to another and reuse the data, it is neither necessary nor proportionate to require that also electronic communications data is subject to Art. 20 GDPR.

Data "provided" by the data subject: As stated above, the wording of "provided" by the data subject to a controller was deliberately chosen over "processed". In this context, traffic and location data is not specifically "provided" by the data subject as the data subject only initiates the communication process. Consequently, traffic and location data is only produced at the time of signalisation within the telecommunication network. In particular, location data does not refer to the location of the individual but to the location of the telecommunication infrastructure (e.g. cell

towers). If any, only the number of the receiving entity can be considered as "provided" as this one has been provided by dialing. However, traffic and location data are created as consequence of standardised protocols and do not depend on the intent of the data subject.

Processing is based on consent or contract pursuant to Art. 6 (1)(b): The collection of location and traffic data is based on specific legal bases in the e-Privacy Directive. Data is rarely processed on the basis of consent or contract, as only certain provisions allow the controller to do so. However, also in these cases the collection and processing of data is specifically allowed under Union or Member State law and falls therefore outside the scope. Furthermore, it is unclear what the implications for the data subject and the new data controller are, given the obligation to delete respective data according to the e-Privacy Directive. An extensive interpretation would therefore collide with data protection in the electronic communication sector as laid down by national law as well as the e-Privacy Directive/ proposed Regulation.

Exceptions and conflicting legal norms: In case such data would be considered as data "provided" by the data subject, the denial of such transfer could be justified under Article 20 (4) as it would violate business and trade secrets and thus "the rights and freedoms of others", especially the data protection rights of the receiving entity.

Conclusion: As a consequence, we believe that the controller is not obliged to provide any data, which has been generated automatically by the service while the data subject is using the service (e.g. logfiles, traffic and location data).

Summary conclusion of the interpretation of data "provided" to the controller
An interpretation of Art. 20 should stick closely to its wording, in order to not contradict the intention of the European legislator as well as take the purpose and goal of the provision into account.

"data provided to a controller"

- Only refers to the data which the data subject controls and accesses on its own (e.g. photos, emails during the performance of the contract and
- Does **not** mean usage data and data necessary for the conclusion of the contract.
    - In any case if usage data were to be included, it could **only** encompass data which is closely linked to the service.
    - The controller is **not** obliged to provide any data, which has been generated automatically by the service while the data subject is using the service (such as logfiles, traffic and location data).

3.3 Processing based on consent and contract

The burden on the new data controller to analyse the data provided by the data subject in terms of whether it contains information that goes beyond the consent or contractual obligations is overly cumbersome and creates legal uncertainties. If the data is not covered by the consent given by the data subject or contractual obligations, the controller has no right to process such data. Since processing starts with the storing of data, the analysis of the data by the controller would already be illegal. In addition, the described practice to hand over full sets of data to further investigate whether all the data points are actually needed is very alarming from a data privacy perspective.

Furthermore, in all discussions on the data portability right as well as in the examples provided by the WP29, the controller-customer relationship is emphasised. However, the wording "the person concerned" could possibly include also the employer-employee relationship.

Example: Employees' Data
Question: It should be clarified whether employees' data is equally within the scope of Art. 20 GDPR. This would avoid misunderstandings and misinterpretations at an early stage.

Bitkom considerations:
Purpose and goal of Art.20 GDPR (see also 2.1): If one considers Art. 20 as electronic version of Art. 15 and takes the goal and purpose of the provision into account - to enable a data subject to electronically transfer personal data from one service provider to another - the scope of application for employees can be already reduced significantly.

Processing based on consent or contract: The additional condition, that the employee has provided the data within the framework of a given consent or contract pursuant to Article 6 (1)(a), will only apply to a part of the data processing in the employment relationship. On the basis of consent, only personal data that is not required for the performance of the employment relationship (e.g. voluntary bonus program or private mobile phone use) can possibly be considered here. Since the scope of using consent as legal basis in the employment relationship is very limited, the majority of data processing operations are likely to be based on Art. 6 (1)(b) or (c).

Exception of Art. 20 (3) S. 2 GDPR: In the context of Art. 6 (1)(b) or (c), it should be considered that the employer processes employees' personal data in many cases due to public law requirements (e.g. German Social Security Code (SGB IV) or German Income Tax Act (EStG))[1]. This processing is "necessary for the performance of a task in the public interest". Therefore, Art. 20 (3) GDPR limits the scope of application and should be taken into account.

Conclusion: As a consequence, we believe that employees' data falls outside the scope of Art. 20 GDPR.

[1] For illustrative purposes, we add a small excerpt of provisions which an employer has to consider when processing data. These are by no means all provisions an employer has to take into account.

Annex A

Beispiele für öffentlich-rechtliche Vorschriften, nach denen ein Arbeitgeber Daten eines Arbeitnehmers verarbeiten muss.

Examples of public provisions which require an employer to process data of an employee.

§ 28a SGB IV (Aufstellung der wichtigsten Meldungen)[1]

DEÜV[2]-Meldung **allgemein**

(1) Der Arbeitgeber oder ein anderer Meldepflichtiger hat der Einzugsstelle für jeden in der Kranken-, Pflege-, Rentenversicherung oder nach dem Recht der Arbeitsförderung kraft Gesetzes Versicherten

1. bei Beginn der versicherungspflichtigen Beschäftigung,

2. bei Ende der versicherungspflichtigen Beschäftigung,

3. bei Eintritt eines Insolvenzereignisses,

4. (weggefallen)

5. bei Änderungen in der Beitragspflicht,

6. bei Wechsel der Einzugsstelle,

7. bei Anträgen auf Altersrenten oder Auskunftsersuchen des Familiengerichts in Versorgungsausgleichsverfahren,

8. bei Unterbrechung der Entgeltzahlung,

9. bei Auflösung des Arbeitsverhältnisses,

10. auf Anforderung der Einzugsstelle nach § 26 Absatz 4 Satz 2,

11. bei Antrag des geringfügig Beschäftigten nach § 6 Absatz 1b des Sechsten Buches auf Befreiung von der Versicherungspflicht,

12. bei einmalig gezahltem Arbeitsentgelt,

13. bei Beginn der Berufsausbildung,

14. bei Ende der Berufsausbildung,

15. bei Wechsel von einem Beschäftigungsbetrieb im Beitrittsgebiet zu einem Beschäftigungsbetrieb im übrigen Bundesgebiet oder umgekehrt,

16. bei Beginn der Altersteilzeitarbeit,

17. bei Ende der Altersteilzeitarbeit,

---

1 §28 Volume IV of German Social Insurance Code (SGB)
2 Data Collection and Transmission Act (DCTA/DEÜV)

18. bei Änderung des Arbeitsentgelts, wenn die in § 8 Absatz 1 Nummer 1 genannte Grenze über- oder unterschritten wird,

19. bei nach § 23b Absatz 2 bis 3 gezahltem Arbeitsentgelt oder

20. bei Wechsel von einem Wertguthaben, das im Beitrittsgebiet und einem Wertguthaben, das im übrigen Bundesgebiet erzielt wurde,

eine Meldung zu erstatten.

Jahresmeldung

2) Der Arbeitgeber hat jeden am 31. Dezember des Vorjahres Beschäftigten nach Absatz 1 zu melden (Jahresmeldung).

Jahresmeldung Unfallversicherung

(2a) Der Arbeitgeber hat für jeden in einem Kalenderjahr Beschäftigten, der in der Unfallversicherung versichert ist, zum 16. Februar des Folgejahres eine besondere Jahresmeldung zur Unfallversicherung zu erstatten. Diese Meldung enthält über die Angaben nach Absatz 3 Satz 1 Nummer 1 bis 3, 6 und 9 hinaus folgende Angaben:

1. die Mitgliedsnummer des Unternehmers;

2. die Betriebsnummer des zuständigen Unfallversicherungsträgers;

3. das in der Unfallversicherung beitragspflichtige Arbeitsentgelt in Euro und seine Zuordnung zur jeweilig anzuwendenden Gefahrtarifstelle.

Meldung für landwirtschaftliche Berufsgenossenschaft

Die Meldungen enthalten für jeden Versicherten insbesondere

1. seine Versicherungsnummer, soweit bekannt,

2. seinen Familien- und Vornamen,

3. sein Geburtsdatum,

4. seine Staatsangehörigkeit,

5. Angaben über seine Tätigkeit nach dem Schlüsselverzeichnis der Bundesagentur für Arbeit,

6. die Betriebsnummer seines Beschäftigungsbetriebes,

7. die Beitragsgruppen,

8. die zuständige Einzugsstelle und

9. den Arbeitgeber.

Zusätzlich sind anzugeben

1. bei der Anmeldung
a) die Anschrift,

b) der Beginn der Beschäftigung,

c) sonstige für die Vergabe der Versicherungsnummer erforderliche Angaben,

d) die Angabe, ob zum Arbeitgeber eine Beziehung als Ehegatte, Lebenspartner oder Abkömmling besteht,

e) die Angabe, ob es sich um eine Tätigkeit als geschäftsführender Gesellschafter einer Gesellschaft mit beschränkter Haftung handelt,

f) die Angabe der Staatsangehörigkeit,

2. bei allen Entgeltmeldungen

a) eine Namens-, Anschriften- oder Staatsangehörigkeitsänderung, soweit diese Änderung nicht schon anderweitig gemeldet ist,

b) das in der Rentenversicherung oder nach dem Recht der Arbeitsförderung beitragspflichtige Arbeitsentgelt in Euro,

c) (weggefallen)

d) der Zeitraum, in dem das angegebene Arbeitsentgelt erzielt wurde,

e) Wertguthaben, die auf die Zeit nach Eintritt der Erwerbsminderung entfallen,

f) (weggefallen)

g) (weggefallen)

h) (weggefallen)

3. (weggefallen)

4. bei der Meldung nach Absatz 1 Satz 1 Nummer 19

a) das Arbeitsentgelt in Euro, für das Beiträge gezahlt worden sind,

b) im Falle des § 23b Absatz 2 der Kalendermonat und das Jahr der nicht zweckentsprechenden Verwendung des Arbeitsentgelts, im Falle der Zahlungsunfähigkeit des Arbeitgebers jedoch der Kalendermonat und das Jahr der Beitragszahlung.

Zahlstellenmeldung

(3a) Der Arbeitgeber oder eine Zahlstelle nach § 202 Absatz 2 des Fünften Buches kann in den Fällen, in denen für eine Meldung keine Versicherungsnummer des Beschäftigten oder Versorgungsempfängers vorliegt, im Verfahren nach Absatz 1 eine Meldung zur Abfrage der Versicherungsnummer an die Datenstelle der Rentenversicherung übermitteln; die weiteren Meldepflichten bleiben davon unberührt. Die Datenstelle der Rentenversicherung übermittelt dem Arbeitgeber oder der Zahlstelle unverzüglich durch Datenübertragung die Versicherungsnummer oder den Hinweis, dass die Vergabe der Versicherungsnummer mit der Anmeldung erfolgt.

Sofortmeldung

(4) Arbeitgeber haben den Tag des Beginns eines Beschäftigungsverhältnisses spätestens bei dessen Aufnahme an die Datenstelle der Rentenversicherung nach Satz 2 zu melden, sofern sie Personen in folgenden Wirtschaftsbereichen oder Wirtschaftszweigen beschäftigen:

1. im Baugewerbe,

2. im Gaststätten- und Beherbergungsgewerbe,

3. im Personenbeförderungsgewerbe,

4. im Speditions-, Transport- und damit verbundenen Logistikgewerbe,

5. im Schaustellergewerbe,

6. bei Unternehmen der Forstwirtschaft,

7. im Gebäudereinigungsgewerbe,

8. bei Unternehmen, die sich am Auf- und Abbau von Messen und Ausstellungen beteiligen,

9. in der Fleischwirtschaft.

Die Meldung enthält folgende Angaben über den Beschäftigten:

1. den Familien- und die Vornamen,

2. die Versicherungsnummer, soweit bekannt, ansonsten die zur Vergabe einer Versicherungsnummer notwendigen Angaben (Tag und Ort der Geburt, Anschrift),

3. die Betriebsnummer des Arbeitgebers und

4. den Tag der Beschäftigungsaufnahme.

Die Meldung wird in der Stammsatzdatei nach § 150 Absatz 1 und 2 des Sechsten Buches gespeichert. Die Meldung gilt nicht als Meldung nach Absatz 1 Satz 1 Nummer 1.

(4a) Der Meldepflichtige erstattet die Meldungen nach Absatz 1 Satz 1 Nummer 10 an die zuständige Einzugsstelle. In der Meldung sind insbesondere anzugeben: 1.

die Versicherungsnummer des Beschäftigten,

2.die Betriebsnummer des Beschäftigungsbetriebes,

3. das monatliche laufende und einmalig gezahlte Arbeitsentgelt, von dem Beiträge zur Renten-, Arbeitslosen-, Kranken- und Pflegeversicherung für das der Ermittlung nach § 26 Absatz 4 zugrunde liegende Kalenderjahr berechnet wurden.

Berufsständische Versorgungseinrichtung

11) Der Arbeitgeber hat für Beschäftigte, die nach § 6 Absatz 1 Satz 1 Nummer 1 des Sechsten Buches von der Versicherungspflicht befreit und Mitglied in einer berufsständischen Versorgungseinrichtung sind, der Annahmestelle der berufsständischen Versorgungseinrichtungen monatliche Meldungen zur Beitragserhebung zu erstatten. Absatz 10 Satz 2 gilt entsprechend. Diese Meldungen enthalten für den Beschäftigten

1. die Mitgliedsnummer bei der Versorgungseinrichtung oder, wenn die Mitgliedsnummer nicht bekannt ist, die Personalnummer beim Arbeitgeber, den Familien- und Vornamen, das Geschlecht und das Geburtsdatum,

2. den Zeitraum, für den das Arbeitsentgelt gezahlt wird,

3. das beitragspflichtige ungekürzte laufende Arbeitsentgelt für den Zahlungszeitraum,

4. das beitragspflichtige ungekürzte einmalig gezahlte Arbeitsentgelt im Monat der Abrechnung,

5. die Anzahl der Sozialversicherungstage im Zahlungszeitraum,

6. den Beitrag, der bei Firmenzahlern für das Arbeitsentgelt nach Nummer 3 und 4 anfällt,

7. die Betriebsnummer der Versorgungseinrichtung,

8. die Betriebsnummer des Beschäftigungsbetriebes,

9. den Arbeitgeber,

10. den Ort des Beschäftigungsbetriebes,

11. den Monat der Abrechnung.

Soweit nicht aus der Entgeltbescheinigung des Beschäftigten zu entnehmen ist, dass die Meldung erfolgt ist und welchen Inhalt sie hatte, gilt Absatz 5.

B § 39 Lohnsteuerabzugsmerkmale EStG[3]

(ELStAM)

4) Lohnsteuerabzugsmerkmale sind

1. Steuerklasse (§ 38b Absatz 1) und Faktor (§ 39f),

2. Zahl der Kinderfreibeträge bei den Steuerklassen I bis IV (§ 38b Absatz 2),

3. Freibetrag und Hinzurechnungsbetrag (§ 39a),

4. Höhe der Beiträge für eine private Krankenversicherung und für eine private Pflege-Pflichtversicherung (§ 39b Absatz 2 Satz 5 Nummer 3 Buchstabe d) für die Dauer von zwölf Monaten, wenn der Arbeitnehmer dies beantragt,

5. Mitteilung, dass der von einem Arbeitgeber gezahlte Arbeitslohn nach einem Abkommen zur Vermeidung der Doppelbesteuerung von der Lohnsteuer freizustellen ist, wenn der Arbeitnehmer oder der Arbeitgeber dies beantragt.

[3] § 39 of the German Income Tax Law (EStG).