

PROTECTION OF SECRECY WHERE THIRD PARTIES ARE INVOLVED

Position statement

22. January 2021

Gender Notice:

For reasons of better readability, the simultaneous use of the language forms female, diverse and male (w/d/m) in this text has been dispensed with. All personal terms apply equally to all genders.

**IMPRINT****Publisher**

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
Budapester Straße 31
10787 Berlin

T 030 . 26 36 77 60
F 030 . 26 36 77 63

bvd-gs@bvdnet.de
www.bvdnet.de

Dear Ms. von Bothmer, Ladies and Gentlemen,

Thank you for your invitation to contribute our opinion on the above draft law. We are pleased to herewith comply.

The Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) [Association of Data Protection Officers of Germany] is the professional organisation of data protection officers. The statutory task of the BvD constitutes the promotion of the interest of company and official data protection officers in data protection and data security through appropriate state of the art measures.

The approx. 900 data protection officers in the BvD attend to several thousand companies, authorities and institutions and are the direct contact persons for employees and customers of these companies.

We will restrict our comment on aspects we encounter in the course of practical work of data protection officers, also offering data protection advice to professionals subject to a professional duty to secrecy and to the threat of prosecution in the event of unauthorised disclosure. We welcome the BMJV [Federal Ministry of Justice and Consumer Protection] taking up this sensitive topic, thereby guarding the interest of companies / citizens who approach professional groups and must have the confidence of trusting these with the details of their personal life or company secrets these groups require for optimal provisioning of their services. But including also the interests of professionals who need legal certainty when commissioning specialists, especially for the provisioning of state of the art IT services.

Attorneys, tax consultants, auditors, doctors, certified youth counsellors, state- approved social workers etc. currently still find themselves in a statutory grey area when they entrust external specialists with the maintenance of their IT systems, without ability to obtain the express consent of their clients / patients in this regard.

In the opinion of the BvD, the BMJV draft bill could clarify the hitherto not unequivocally defined "unauthorised disclosure" elements of a case in a way to allow the involvement of external specialists without detracting from the requisite element of professional trust. We would, however, also like to point out practical situations which the envisaged formulations will not resolve and may in cases even aggravate.

We will first comment in general on the participation of the legislative organs in federal government and states, followed by comment on specific expositions in the concrete draft bill in the second part.

I GENERAL NOTES

1. Consistency with European law

Note: Since the GDPR does not, pursuant to Art. 26 Para. 2 TFEU , Art. 2 Para GDPR and Recital 13 Clause 2 of the GDPR, allow restrictions of free data traffic outside the GDPR, explanations should be given as to why § 203 StGB- E [Draft Criminal Code] will not contradict these European law provisions.

Grounds: There is a debate within the framework of the GDPR whether § 203 StGB [Criminal Code] is still admissible under European law, since it restricts the involvement of service providers in personal data processing over and above the provisions of Art. 28 GDPR.

Recommendation: This topic should be addressed within the framework of deliberations on the compatibility with EU law under the statement of grounds, Part A, Clause V, not to jeopardise the legal basis of this statutory amendment.

2. Requirement of uniform formulation for different occupational groups

The proposed changes to the provisions for attorneys and notaries under vocational law should in principle be worded the same for the other vocational law provisions for which the BMJV is not responsible (e.g. doctors, chemists, auditors, tax consultants, recognised youth counsellors, state-approved social workers). This would, especially in the case of professionals with multiple qualifications, as often found among attorneys, tax consultants and auditors, prevent legal uncertainty when service providers become involved, as may be the case when requirements differ.

Different wording of state laws could, for the other vocational groups given in § 203 Para. 1 StGB under the responsibility of the different states (e.g. in the health sector) lead to confusion of diverse and impractical demands. The BvD would here call for coordinated wording across all vocational groups, to ensure involvement of third parties with no legal uncertainties. Without forestalling the detailed notes under Point II., the requirement that attorneys, notaries and patent attorneys should, for instance, commission the involved service providers or persons in writing, whilst the written form requirement will not, as per § 203 Para. 1 StGB, apply to other occupational groups, result in a differentiation that is neither traceable nor practical.

Since, however, some occupational groups named under § 203 Para. 1 StGB are not and will not be subject to special rules under vocational law, the statement of grounds should at least explain that the amendment in § 203 StGB as envisaged under the draft bill constitutes merely the authority to disclose the involvement of service providers and that any arrangements under vocational law would only be a welcome supplement. Violation of the requirements under vocational law would then have consequences only under vocational law, not criminal consequences.

3. Description of the differences compared to data protection requirements

The involvement of service providers for the processing personal data is subject to the requirements of the Data Protection Act, which will require the conclusion of an agreement on the processing of order data between client and contractor, pursuant to § 11 BDSG (in future Art. 28 GDPR). The contractor shall carefully select his service provider (§ 11 Para. 2 Clause 1 BDSG, or Art. 28 Para.1 GDPR); the service provider shall process exclusively the personal data defined in the instructions (§ 11 Para. 3 BDSG, or Art. 28 Para. 3 Clause 2 lit. a, Art. 29 GDPR) and the client shall regularly check that the agreed protective measures are complied with (§ 11 Para. 2 Cl. 4 BDSG) or the contractor shall support the client in this by providing proof of compliance with the agreed obligations (Art. 28 Para. 3 lit. h GDPR).

The limits to the obligations within the framework of authorised disclosure, or whether simply the proper order processing compliant with the specific data protection provisions will meet the facts of a case under § 203 StGB-E or the arrangements under vocational law, remains uncertain. Clarification in the statement of grounds would be very useful in this respect.

A situation where the involvement of a service provider is not subject to data protection regulations is conceivable only in cases where confidentiality towards companies is mandated under vocational law without reference to a person, e.g. when a veterinarian commissions the disposal of vaccination certificates for the animals of an Agrar GmbH.

4. Attention to practical design

The draft wording obviously assumes that the involved service providers will be natural persons ("participating persons"). However, as also explained in the statement of grounds in Part A II. 1. A) (Page 18), a company would normally be commissioned and such company would then assign execution of the order to its employees. In such situations, arrangements where the person obligated to secrecy will, for instance, directly place a participating person under obligation of secrecy would not be feasible in practice.

The arrangement should rather be that disclosure to included companies will be permissible with the proviso that employees becoming privy to data subject to professional secrecy be placed under contractual obligation to secrecy.

5. Note on independent vocations completing their tasks not bound by directives

The BvD would welcome the particular vocational laws containing clarifications that the execution of tasks specified under a specific vocational law will not be subject to directives pursuant to § 11 BDSG or Art. 28 GDPR, since professions such as attorney, auditor, tax consultant, external data protection officer or company medical officer are not bound by directives. These professions cannot fulfil their sociopolitical tasks, explicitly defined as their responsibility as independent bodies of the judiciary, the fiscal system, business and health care etc. unless they are not bound by directives and that they cannot be restricted in the use of personal data by restrictions by patients, clients etc. The interests of the latter will be adequately protected under vocational law provisions for secrecy (subject to penalties) and no agreement on order data processing will in these cases be required (see also 6th Activity report of the Bavarian Data Protection Authority for 2013 / 2014, Clause 5.6).

II NOTES ON THE PROPOSED CHANGES

1. § 203 Para. 3 StGB-E

The BvD appreciates the phrasing in the revised version, enabling the involvement of further persons also indirectly deployed for tasks in the interest of persons obligated to secrecy. This will according to the statement of grounds in Part A II. 1 a) of § 203 Para. 3 StGB-E, allow the involvement of external attorneys by hospitals for the collection of outstanding fees or the commissioning of tax consultants by chemists for their accounting, with no legal uncertainties.

2. § 203 Para. 4 No. 1 StGB-E

Selection, obligation and supervision

Note: The envisaged culpability of persons bound to professional secrecy in cases of inadequate care with the selection of service providers and their supervision should also take into account whether the deployed service provider is also bound by an obligation to secrecy under vocational law, already punishable in the event of unauthorised disclosure.

Grounds: According to Part A Clause II 1 c) and Part B of § 43f BRAO-E [Draft Federal Lawyers' Act] of the draft legislation statement of grounds, these envisaged regulations for services will also include, for instance, postal or tax consulting services. The selection and supervision of services already subject to admissibility procedure under public law and where violation of obligations to secrecy is punishable already appears virtually impossible in practice. This may, for instance, affect tax consultants doing a chemist's bookkeeping, attorneys collecting fees patients owe hospitals, attorneys sending letters to clients via postal services or telephonic scheduling by a psychologist. How should a person bound to professional secrecy perform such meticulous selection unless via present approval criteria of the Federal Network Agency for Telecommunications and Postal Services or the approval procedures of the Chamber for attorneys, auditors and tax consultants, not to mention the effective supervision of these service providers?

Recommendation: It should be made clear by appropriately phrasing § 203 Para. 3 StGB-E or by explanations under the statement of grounds under Part A Clause II 1c) and Part B under § 43f BRAO-E, that these prerequisites to the meticulous selection, obligation to secrecy and supervision will suffice for the selection of service providers bound by admission requirements under public law and punishable obligation to secrecy.

3. § 203 Para. 4 No. 1 StGB-E

Extension to the external data protection officer of the deployed service provider

Note: The extension of culpability to participating persons would also include external data protection officers of a deployed service provider, even should he not be accordingly informed in advance.

Grounds: It is not evident from the wording that a participating person cannot be held culpable unless he is obligated to secrecy in advance.

Recommendation: § 203 Para. 4 StGB-E should be supplemented stating that the participating person must be informed that the data being processed is subject to prohibition of unauthorised disclosure.

4. § 204 Para. 2 StGB

We suggest examining the extent of corresponding amendments of § 204 Para. 2 StGB, which refers to § 203 Para. 4 StGB - for instance by a more specific reference to § 203 Para. 4 No. 2 StGB-E.

The examples of the following notes apply only to phrasing for the Federal Code for the Legal Profession; they will, however, also apply verbatim to the analogous or homonymous proposals for amendment of the Federal Code on Notaries, the Patent Attorney Code, the Tax Consultancy Act, the Independent Auditors' Code or other provisions of the vocational law which other Federal ministries or provincial governments are handling.

5. § 43a Para. 2 BRAO-E, supplements

No notes. The written form requirement concerning secrecy is also relevant in practice to persons directly deployed in the chambers, practices etc. under work contracts etc., for instance in conjunction with present obligations to data secrecy pursuant to § 5 BDSG, and should be implemented.

6. § 43f Para. 2 Clause 1 BRAO-E

Reference is made to the subject matter discussed under Clause 1. 2. in respect of the selection and supervision of service providers appointed by persons bound to professional secrecy.

Hospitals, chemists, occupational psychologists etc. must, without further investigation or supervisory measures, be able to rely on other persons bound to professional secrecy whom they appoint for his purposes, to treat information protected under vocational law that they may become privy to within the framework of such deployment with the required confidentiality. Any supervisory measures by a client could jeopardise the obligation of secrecy towards other patients, clients etc. of the deployed person bound to professional secrecy.

7. § 43f Para. 3 Clause 1 BRAO-E

Formal requirements when deploying services

Note: We welcome a contractual basis as prerequisite for the involvement of service providers. The formal requirements should, however, be limited to the essential. The provision in § 43f Para. 2 BRAO-E that the participating persons must be commissioned through a written contract with the service provider burdens the participating parties with an unnecessary administrative effort without adding value to the legal interests to be protected.

Grounds: Under present provisions on consideration of evidence, commissioning in text form satisfies the requirements for verification and protection. The strict written form requirement under § 11 BDSG contradicts European law since it creates another hurdle to permissibility, as opposed to the requirements under Art. 17 Para. 4 Directive 95/46 EC (see Kramer in PinG 2014, 77 (79)).

The demands for a statutory, mandatory written form requirement exceed the objective of creating a verifiable base. Verification may also be provided by agreements in text form (§ 126b BGB [Civil Code]), communicated by e-mail, for instance. Art. 28 Para. 9 GDPR, intended to enter into effect on 25 May, 2018, provides that commissioning electronically will suffice for order processing. It appears contradictory that the justification of this statutory amendment includes the convenience of using Internet services ("Cloud offers") whilst also enforcing printing and mailing of the particular contractual documentation. The objective of allowing persons under obligation of secrecy to use Cloud service providers would be thwarted by a strict written form as described in §126 BGB ff.

We point out that also for the vocational groups under § 203 Para.1 StGB, not subject to an own professional code of conduct, that this statutory initiative will change using the same wording, the involvement of a service provider will not be subject to this stringent prescribed form.

Recommendation: Amendment of "written" to "documented in writing or other form (text form)".

8. § 43f Para. 3 Clause 2 No. 2 BRAO-E **Obligation of required information**

Note: The requirement to obligate a service provider to limit his exposure to external secrets to that which will be contractually required must not result in the need for a person bound to professional secrecy to always before commissioning a service provider define the scope and data the latter will need.

Grounds: Especially when other persons bound to professional secrecy such as attorneys, auditors and tax consultants are commissioned, including also the consultation of specialists for expert opinions, these must not be bound by directives when bringing their professional competence to bear on the assessment of information, i.e. they must in individual cases also be allowed to collect additional data and information on own volition.

Recommendation: This special situation should be explained in the statement of grounds in the special section under § 203 Para. 3 StGB-E in cases where involved parties are also bound to professional secrecy.

9. § 43f Para. 3 Clause 2 No. 3 BRAO-E

Obligation to secrecy of participating persons of (further) service providers

Note: The phrasing requiring the service provider to obligate other persons he may involve for fulfilment of his contract to secrecy, in writing, is unclear since, phrased in this way, it cannot be implemented in practice.

Grounds: Should, for instance, a call centre operating for a doctor appoint a subcontractor (call centre 2), then the initially commissioned call centre will have no way of accessing specific staff appointed at call centre 2 in order to make a specific arrangement for obligation to secrecy.

Recommendation: It must suffice to obligate the service provider, when engaging further service providers, to demand that these obligate their staff to secrecy. Since the service provider is required to provide relevant verification, the written form requirement may be waived. A deployed member of staff could then, for instance, be bound via a pop-up window during remote access to protected data, without the service provider needing to know in advance which member of staff will be supporting the customer.

Proposed phrasing for § 203 Para. 3 Clause 2 No. 3 last main clause BRAO-E by supplementing the word “further” and deleting the words “in writing”:
“ ..; further service providers shall in this case be obligated to bind these persons to secrecy, ~~in writing~~.”

10. § 43f Para. 3 Clause 2 No. 3 BRAO-E

Calling on further persons for fulfilment of the contract

Note: The wording envisages that a service provider will be authorised to call on additional persons for fulfilment of the contract. This phrasing leaves it unclear how the elements of “fulfilment of the contract” of a case should be interpreted.

Grounds: Should, for instance, an attorney appoint an external call centre to answer calls in his absence, then the wording in § 43f Para. 3 Clause 2 No. 3 leaves unanswered the question of the extent to which this arrangement will also apply to the telephone system servicing partner of the call centre. The telephone system servicing partner could thus also see the call numbers of the person bound to professional secrecy whilst busy with services, support or troubleshooting.

Recommendation: It should be explained at least in the statement of grounds that the elements “fulfilment of the contract” of a case relate to only the specific commissioned service.

Dear Ms. von Bothmer, Ladies and Gentlemen,

We trust that our notes will be of use to you in creating a legal framework which will accommodate the interest professionals have in carrying out their statutory tasks in an environment of trust, including also their interest in commissioning qualified service providers.

We will be at your disposal should you have further queries. You are welcome to pass on these comments to ministerial departments participating in the legislative procedure or to publish the comments on your homepage.

Yours sincerely

Thomas Spaeing
Chairman of the BvD Board

About the Professional Association of Data Privacy Germany (BvD) e. V.

With over 30 years of experience, the Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. (Professional Association of Data Protection Officers in Germany) is the oldest lobby group for company and public authority data protection officers and consultants. BvD members are represented in all sectors, especially IT and ICT, industry/production, trade/sales, consulting, and health and social services. As the first point of contact for those affected, BvD members are the point of contact for around five million employees and a large proportion of citizens and consumers. In addition, as constructive solution-oriented data protection experts, they are an important partner for the responsible company management.

The association's board members, all heads of working groups, committees and regional groups of the BvD contribute their practical experience to the association's work free of charge. With the founding of the European umbrella organization EFDPO (www.efdpo.eu), the BvD has set the course for increased networking and communication at the EU level.

