Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDPR Good Practices - XI

Confidentiality agreement

TABLE OF CONTENTS

Confidentiality agreement

The previous data protection law provided for a so-called „confidentiality obligation“. Section 5 Federal Data Protection Act (FDPA)(former version)(german: Bundesdatenschutzgesetz – BDSG) statues: „Persons employed in data processing shall not collect, process or use personal data without authorization (confidentiality). Such persons, when employed by private bodies, shall be obligated when taking up their duties to maintain confidentiality. The obligation of confidentiality shall continue after their employment ends.”

A comparably clear and unambiguous regulation is no longer contained in the GDPR. In this respect, the question arises for data processing companies whether the classical confidentiality agreement still has a future. If such a formal obligation on employees remains necessary, an update of the former agreements may be necessary.

This guideline is intended to provide an overview of the nature and content of a confidentiality agreement. A corresponding sample is attached.

Please note: The texts in italics refer to German law.

1. Confidentiality agreement

1.1. Agreement as a valid organisational measure

The confidentiality agreement is more than just a ritual. It has a clear warning and teaching function. In the context of the documentation and compliance obligations of art. 5 para. 2 GDPR (Accountability), the controllers obligation to conclude such agreement continues to be regarded as an effective means of ensuring compliance with data protection regulations from the outset.

This can be seen, among other things, in the regime of data processing on behalf, which in art. 28 para. 3 letter b GDPR expressly provides for the agreement of confidentiality, at least in the case of the processor, as an obligatory content of the contract for data processing on behalf.

In addition, art. 32 para. 4 GDPR stipulates that both, data controllers and processors, must take steps to ensure that persons employed in data processing act only on the instructions of the controller. Art. 29 GDPR also refers to this clearly instruction-dependent processing. This includes making clear reference to the importance and scope of data protection rules and making employees aware of any risks of violations of the law.

The national legislator in Germany has maintained the formal agreement in the context of the implementation of Directive 2016/680/EU on data protection in the police and judiciary. In this respect, section 53 BDSG as amended even uses the traditional term of confidentiality. What is right in the public sector can therefore only be correct in the non-public sector.

In the case of vocational and professional law, the omission of an agreement for persons employed in data processing according to section 203 para. 4 sentence 2 no. 1 German Criminal Code (Strafgesetzbuch – StGB) may even be punishable if the participating person discloses unauthorized third-party secrets.

1.2. Content and consequences

The obligation of confidentiality refers directly to art. 5 para. 1 letter f GDPR („integrity and confidentiality“) and thus to

- >> appropriate security of the personal data;
- >> protection against unauthorised or unlawful processing,
- >> protection against accidental loss,
- >> protection against destruction or damage.

This regulation is flanked by art. 32 para. 2 GDPR, according to which, among other things,

- >> unauthorised disclosure of, or
- >> unauthorised access to personal data transmitted, stored or otherwise processed is to be prevented.

Corresponding explanations can also be useful in sector-specific data protection law, if, for example, the privacy of telecommunications (section 88 Telecommunications Act - TKG), social secrecy (e.g. section 78 para. 1 sentence 3 German Social Code - SGB X) or private secrets (e.g. section 203 StGB) are relevant. Meanwhile, the obligation does not have a constitutive effect, i.e. the legal requirements of data protection law apply even without individual classification.

1.3. Form and time

Since the GDPR contains no obligation for a confidentiality agreement, no specific form is envisaged. However, it is in the interest of evidence to choose the written form together with a handwritten signature. It is also conceivable to make and document the commitment at the end of an eLearning process or within the framework of a digital instruction process.
The obligation only fulfils its purpose if it takes place before the start of the data processing activity. When entering into an employment or service relationship, the agreement may be signed together with the contractual documents, but care should be taken to ensure that the declaration does not disappear in a mass of documents. In this respect, it is advisable to have at least one separate document - with a copy of the main legal provisions regarding the employee's whereabouts. It may be helpful to hand out a general information sheet or the company policy on data protection.

1.4 Continuity of agreements

There is no need for a new confidentiality agreement under the GDPR. It would lead to unnecessary formalism, especially if there are a large number of employees. Precisely because the obligation does not have a constitutive effect, but only has a warning and instructional function, previous declarations under previous law are just as capable of fulfilling this function.

In the context of training and advising all employees within the meaning of art. 39 para. 1 letter a GDPR, however, it is useful to draw attention to the changes in data protection law in an appropriate form, if necessary by means of a circular letter.

2. Sample

The following sample is intended to provide information on the general principles of data protection in the necessary conciseness. The confidentiality agreement itself makes no direct reference to individual legal norms. This makes it easier to read. Instead, an exemplary selection of relevant legal provisions can be found in the attached annex. Meanwhile, the agreement alone cannot replace comprehensive training.

Confidentiality agreement

The relevant legislation requires that personal data be processed in a manner that ensures the rights of data subjects to the confidentiality and integrity of their data. Therefore, you are only permitted to process personal data to the extent and in the manner it is necessary for compliance with the tasks assigned to you.

Data protection rules prohibit unauthorised or unlawful processing of personal data as well as intentionally or unintentionally violating the security of processing in a manner that results in destruction, loss, alteration, unauthorized disclosure, or unauthorized access.

Violations of the data protection laws may be punishable by fine, penalty or imprisonment. If the data subject incurs material or immaterial damage as a result of a prohibited processing of their personal data, a claim for damages may arise.
A breach of the confidentiality and data protection regulations constitutes a breach of employment contract obligations, which can be punished accordingly.

Optional - Your activity affects telecommunications secrecy. You must not gain knowledge of the content or the specific circumstances of telecommunications beyond what is necessary. You are not allowed to pass on such knowledge to third parties.

Optional - Your activity affects social secrecy. If data is processed that is subject to social secrecy, you must keep it secret to the same extent as the original transmitting body.

Optional - Your activity affects the [legal / medical / etc] confidentiality. You shall participate only as far as necessary, in the professional or administrative activities of a person bound by private secrets. You are prohibited from disclosing unauthorized third-party secrets, especially personal secrets or business or trade secrets.

This confidentiality agreement shall also apply after termination of employment.

Mrs/ Mr	Department / activity
.....	.....

declares that it complies with the applicable data protection regulations with regard to the confidentiality and integrity of personal data.

By signing, you also confirm receipt of a copy of this transcript and attachment.

.....	.....
Place/Date	Obligated person

Annex to the confidentiality agreement

The present selection of legal regulations should give you an overview of the data protection regulations. The presentation is exemplary and by no means complete. Further information on data protection issues can be obtained from the company data protection officer (DPO).

Terminology

Art. 4 nr. 1 GDPR: „**Personal data**“ means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Art. 4 nr. 2 GDPR: „**processing**“ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Principles of processing

Art. 5 nr. 1 letter a GDPR: Personal data shall be processed lawfully, fairly and in a transparent man-

ner in relation to the data subject ('lawfulness, fairness and transparency').

Art. 5 nr. 1 letter f GDPR: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Art. 29 GDPR: The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Art. 32 para. 2 GDPR: In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Art. 33 para. 1 sentence 1 GDPR: In the case of a personal data breach, 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 [...], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Liability

Art. 82 para. 1 GDPR: Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Art. 83 para. 1 GDPR: Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred [...] shall in each individual case be effective, proportionate and dissuasive.

Optional - penal provisions

Section 42 Federal Data Protection Act (FDPA) (german: Bundesdatenschutzgesetz – BDSG)

(1) The following actions done deliberately and without authorization with regard to the personal data of a large number of people which are not publicly accessible shall be punishable with imprisonment of up to three years or a fine:

1. *transferring the data to a third party or*
2. *otherwise making them accessible*

for commercial purposes.

(2) The following actions done with regard to personal data which are not publicly accessible shall be punishable with imprisonment of up to two years or a fine:

1. *processing without authorization, or*
2. *fraudulently acquiring*

and doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

Section 202a para 1 German Criminal Code (StGB): Whoever, without being authorised to do so, obtains access, by circumventing the access protection, for themselves or another, to data which were not intended for them and were specially protected against unauthorised access incurs a penalty of imprisonment for a term not exceeding three years or a fine.

Section 303a para. 1 German Criminal Code (StGB): Whoever unlawfully deletes, suppresses, renders unusable or alters data [...] incurs a penalty of imprisonment for a term not exceeding two years or a fine.

Optional - Telecommunications secrecy

Section 88 Telecommunications Act - TKG

(1) The content of telecommunications and the detailed circumstances thereof, in particular the fact of whether a person is or has been involved in telecommunications traffic, shall be subject to telecommunications secrecy. Telecommunications secrecy shall also cover the detailed circumstances surrounding unsuccessful call attempts.

(2) Whosoever commercially provides or assists in the provision of telecommunications services shall be obliged to maintain telecommunications secrecy. The obligation to maintain secrecy shall also apply after the end of the activity through which such commitment arose.

(3) Any person subject to the obligation according to (2) above shall be prohibited from procuring for himself or other parties any information regarding the content or detailed circumstances of telecommunications beyond that necessary for the commercial provision of telecommunications services. Knowledge of facts which are subject to telecommunications secrecy may only be used for the purpose referred to in sentence 1 above. Use of such knowledge for other purposes, in particular its retransmission to other parties, shall only be admissible insofar as provided for by this Act or any other legal provision and reference is made expressly to telecommunications traffic. The reporting requirement according to §138 of the German Criminal Code (StGB) shall have priority.

(4) Where the telecommunications system is located on board a ship or aircraft, the obligation to maintain secrecy shall not apply in relation to the master or his representative.

Optional – Violation of private secrets

Section 203 German Criminal Code (StGB)

(1) Whoever unlawfully discloses another's secret, in particular a secret relating to that person's personal sphere of life or to a business or trade secret which was revealed or otherwise made known to them in their capacity as

1. a physician, dentist, veterinarian, pharmacist or member of another healthcare profession which requires state-regulated training to engage in the profession or to use the professional title,

2. a professional psychologist with a state-recognised final academic examination,

3. a lawyer, non-lawyer provider of legal services who has been admitted to a bar association, patent attorney, notary, defence counsel in statutorily regulated proceedings, certified pub-

lic accountant, sworn auditor, tax consultant, tax representative, or organ or member of an organ of a law, patent law, accounting, auditing or tax consulting firm,

4. a marriage, family, education or youth counsellor or addiction counsellor working in a counselling agency which is recognised by an authority or body, institution or foundation under public law,

5. a member or agent of a counselling agency recognised under sections 3 and 8 of the Act on Pregnancies in Conflict Situations (Schwangerschaftskonfliktgesetz),

6. a state-recognised social worker or state-recognised social education worker or

7. a member of a private health, accident or life insurance company or a private medical, tax consultant or lawyer invoicing service incurs a penalty of imprisonment for a term not exceeding one year or a fine.

(4) Whoever, without being authorised to do so, reveals another's secret which has become known to them in the exercise or on the occasion of their work as an involved person or in the performance of their duties as data protection officer for the persons referred to in subsections (1) and (2) incurs a penalty of imprisonment for a term not exceeding one year or a fine. [...].

Gesellschaft für Datenschutz
und Datensicherheit e.V.

The contents were created within the GDD working group „GDPR in practice“.

Layout: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Editor:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 2 28 96 96 75 00
Fax: +49 2 28 96 96 75 25
www.gdd.de
info@gdd.de

Status:
Version 1.0 - May 2020