Template Agreement Annex

Processing of personal data on behalf of a controller in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR)

www.bitkom.org

bitkom

Publisher

Bitkom e. V.
Federal Association for Information Technology, Telecommunications and New Media
Albrechtstraße 10 | 10117 Berlin | Federal Republic of Germany

Contact

Susanne Dehmel | Member of Executive Board for Law & Security
T +49 30 27576-223 | s.dehmel@bitkom.org

Editor

Martina Krauss | EU Policy Advisor
T +32 2 60953-16 | m.krauss@bitkom.org

Bitkom working group responsible for this document

Data Protection Working Group

Cover Image

© vadim yerofeyev – iStock.com

This updated edition 1.1 was created in May 2017, based on the EU General Data Protection Regulation (GDPR). It supersedes the previous editions of this guideline. The GDPR must be applied as of 25 May 2018.

We should like to specifically thank the following members of the working group for their contributions to this updated edition:

- Josef Beck, Atos Information Technology GmbH
- Mareike Böddeker, Bertelsmann SE & Co. KGaA
- Sebastian Brüggemann, IBM Deutschland GmbH
- Giovanni Brugugnone, Hewlett-Packard Europa
- Almuth Flunkert, Hewlett-Packard GmbH
- Markus Frowein, Telefónica Germany GmbH & Co. OHG
- Hens Gehrandt, arvato direct services Münster GmbH
- Wulf Kamlah, SKW Schwarz Rechtsanwälte
- Rudi Kramer, Datev eG
- Ilona Lindemann, gkv informatik GbR
- Regina Mühlich, Teqcycle Solutions GmbH
- Karolina Rozek, Robert Bosch GmbH
- Martin Schweinoch, SKW Schwarz Rechtsanwälte
- Sylle Schreyer-Bestmann, CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB
- Andreas Splittgerber, Olswang Germany LLP
- Hendrik Tamm, HSH Soft- und Hardware Vertriebs GmbH
- Florian Thoma, Accenture GmbH
- Christian Wagner, Nokia and Networks GmbH & Co. KG
- Stephan Weinert, Computacenter AG & Co. oHG

The material contributors to the original version of this guideline were Rudi Kramer, Lars Marten Kripko, Ilona Lindemann, Catrin Peter, Hermann-Josef Schwab, Christian Wagner, Stephan Weinert.

The English translation has been provided by Markus Stamm, Nokia Solutions and Networks GmbH & Co. KG.

Instructions for use:

Some parts of the Annex contain alternative wording and clauses, options and fields to be completed by the user. These are emphasised in the text.

- Alternative wording variations are denoted by the designation »Var.« and shaded grey,
- Optional wording is denoted by the abbreviation »Opt.« and shaded blue,
- Clauses that may need to be augmented individually are shaded yellow.

To make transparent the motivation of the template clauses provided, as well as the reasons for the considerations suggested, as applicable, the »Reference Guide« contains further explanations on many of the regulations.

- Sections in the annex template text for which the »Reference Guide« provides such explanations are marked with a blue superscript asterisk (*).

We recommend that users always consult the »Reference Guide« when using the annex template.

Annex [xxx] to the agreement dated [xxx]

concluded by and between xxx

– hereinafter, “Company”–

and xxx

– hereinafter, “Supplier”–

on the processing of personal data on behalf of a controller in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR).

Preamble

This annex details the parties' obligations on the protection of personal data, associated with the processing of personal data on behalf of Company as a data controller, and described in detail in the agreement dated xxx (hereinafter, the "Agreement")*. Its regulations shall apply to any and all activities associated with the Agreement, in whose scope Supplier's employees or agents process Company's personal data (hereinafter, "Data") on behalf of Company as a controller (hereinafter, "Contract Processing")*.

§ 1 Scope, duration and specification of contract processing of Data

The scope and duration and the detailed stipulations on the type and purpose of Contract Processing shall be governed by the Agreement. Specifically, Contract Processing shall include, but not be limited to, the following Data: (Note: If the Agreement is silent on this information, fill in the following table. Otherwise, remove the table and this last clause.)

Type of data	Type and purpose (subject matter) of Contract Processing	Categories of data subjects affected

Except where this annex stipulates obligations beyond the term of the Agreement, the term of this annex shall be the term of the Agreement.

§ 2 Scope of application and responsibilities

(1) Supplier shall process Data on behalf of Company. Such Contract Processing shall include all activities detailed in the Agreement and its statement of work. Within the scope of this annex, Company shall be solely responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Supplier and the lawfulness of having Data processed on behalf of Company. Company shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.

(2) Company's individual instructions on Contract Processing shall, initially, be as detailed in the Agreement. Company shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form*), modifying, amending or replacing such individual instructions by issuing such instructions to the point of contact designated by Supplier. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the statement of work. Company shall, without undue delay*, confirm in writing or in text form any instruction issued orally.

§ 3 Supplier's obligations

(1) Except where expressly permitted by Article 28 (3)(a) of the GDPR, Supplier shall process data subjects' Data only within the scope of the statement of work and the instructions issued by Company. Where Supplier believes that an instruction would be in breach of applicable law, Supplier shall notify Company of such belief without undue delay. Supplier shall be entitled to suspending performance on such instruction until Company confirms or modifies such instruction.

(2) Supplier shall, within Supplier's scope of responsibility, organise supplier's internal organisation so it satisfies the specific requirements of data protection. Supplier shall implement technical and organisational measures to ensure the adequate protection of Company's Data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. Supplier shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. Company is familiar with these technical and organisational measures, and it shall be Company's responsibility that such measures ensure a level of security appropriate to the risk.

Var. 1
With regard to compliance with the protective measures and safeguards agreed upon and their verified effectiveness, parties refer to an approved code of conduct as defined in Article 40 of the GDPR, which Supplier has declared adherence to on dd mm yyyy and whose compliance was verified and confirmed on dd mm yyyy, as documented in exhibit x hereto. (Note: It is likely that this variation will not yet be available in May 2018.)

Var. 2
With regard to compliance with the protective measures and safeguards agreed upon and their verified effectiveness, parties refer to the existing certification valid in accordance with Article 42 of the GDPR, whose compliance Company has verified and confirmed on dd mm yyyy, as documented in exhibit x hereto. (Note: It is likely that this variation will not yet be available in May 2018.)

Var. 3
With regard to compliance with the protective measures and safeguards agreed upon and their verified effectiveness, parties refer to the existing certification issued by [certification body] presented to and sufficient for Company as proof of the appropriate guarantees, as documented in exhibit x hereto.

Supplier reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.

(3) Supplier shall support Company, insofar as is agreed upon by the parties, and where possible for Supplier, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 33 to 36 of the GDPR. (Note: The parties are free to agree upon a remuneration for such support in the agreement.)

(4) Supplier warrants that all employees involved in Contract Processing of Company's Data and other such persons as may be involved in Contract Processing within Supplier's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, Supplier warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contract Processing.

(5) Supplier shall notify Company, without undue delay, if Supplier becomes aware of breaches of the protection of personal data within Supplier's scope of responsibility.

Supplier shall implement the measures necessary for securing Data and for mitigating potential negative consequences for the data subject; the Supplier shall coordinate such efforts with Company without undue delay.

(6) Supplier shall notify to Company the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

(7) Supplier warrants that Supplier fulfills its obligations under Article 32 (1)(d) of the GDPR to implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(8) Supplier shall correct or erase Data if so instructed by Company and where covered by the scope of the instructions permissible. Where an erasure, consistent with data protection requirements, or a corresponding restriction of processing is impossible, Supplier shall, based on Company's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to Company. (Note: The parties are free to agree upon a remuneration for such support in the agreement.)

In specific cases designated by Company, such Data shall be stored or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement. (Note: The parties are free to agree upon a remuneration for such support in the agreement.)

(9) Supplier shall, upon termination of Contract Processing and upon Company's instruction, return all Data, carrier media and other materials to Company or delete the same.

Opt.: In case of testing and discarded material no instruction shall be required.

Opt.: Company shall bear any extra cost caused by deviating requirements in returning or deleting data.*

(10) Where a data subject asserts any claims against Company in accordance with Article 82 of the GDPR, Supplier shall support Company in defending against such claims, where possible. (Note: The parties are free to agree upon a remuneration for such support in the agreement.)

§ 4 Company's obligations

(1) Company shall notify Supplier, without undue delay, and comprehensively, of any defect or irregularity with regard to provisions on data protection detected by Company in the results of Supplier's work.

(2) Section 3 para. 10 above shall apply, mutatis mutandis, to claims asserted by data subjects against Supplier in accordance with Article 82 of the GDPR. (Note: The parties are free to agree upon a remuneration for such support in the agreement.)

(3) Company shall notify to Supplier the point of contact for any issues related to data protection arising out of or in connection with the Agreement.

§ 5 Enquiries by data subjects

(1) Where a data subject asserts claims for rectification, erasure or access against Supplier, and where Supplier is able to correlate the data subject to Company, based on the information provided by the data subject, Supplier shall refer such data subject to Company. Supplier shall forward the data subject's claim to Company without undue delay. Supplier shall support Company, where possible, and based upon Company's instruction insofar as agreed upon. Supplier shall not be liable in cases where Company fails to respond to the data subject's request in total, correctly, or in a timely manner.

§ 6 Options for documentation

(1) Supplier shall document and prove to Company Supplier's compliance with the obligations agreed upon in this exhibit by appropriate measures.

Opt.: Where specific types of documentation and proof can be identified, with regard to compliance with the obligations agreed upon, Supplier may make available to Company the following information:

Var. 1 conducting an own self-audit

Var. 2 internal compliance regulations including external proof of compliance with these regulations

Var. 3 certifications on data protection and/or information security (e.g. ISO 27001)

Var. 4 codes of conduct approved in accordance with Article 40 of the GDPR

Var. 5 certifications in accordance with Article 42 of the GDPR

Var. 6 Company and Supplier agree that documentation and proof can also be submitted through the production of the following documentation and/or certifications:

- ...
- ...

(2) Where, in individual cases, audits and inspections by Company or an auditor appointed by Company are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with Supplier's operations, upon prior notice, and observing an appropriate notice period. Supplier may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other customers and the confidentiality of the technical and organisational measures and safeguards implemented. Supplier shall be entitled to rejecting auditors which are competitors of Supplier.

Var. Company hereby consents to the appointment of an independent external auditor by Supplier, provided that Supplier provides a copy of the audit report to Company.

Supplier shall be entitled to requesting a remuneration for Supplier's support in conducting inspections where such remuneration has been agreed upon in the Agreement. Supplier's time and effort for such inspections shall be limited to one day per calendar year, unless agreed upon otherwise.

(3) Where a data protection supervisory authority or another supervisory authority with statutory competence for Company conducts an inspection, para. 2 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

§ 7 Subcontractors (further processors on behalf of Company)

(1) Supplier shall use subcontractors as further processors on behalf of Company only where approved in advance by Company.

(2) A subcontractor relationship shall be subject to such consent of Supplier commissioning further supplier or subcontractors with the performance agreed upon in the Agreement, in whole or in part. Supplier shall conclude, with such subcontractors, the contractual instruments necessary to ensure an appropriate level of data protection and information security.

Var. 1
Supplier will conduct the performance agreed upon, or the parts of the performance identified below, using the subcontractors enumerated below:

Name and address of the subcontractor	Description of the affected parts of performance
xxx	xxx

Supplier shall obtain Company's consent prior to the use of new or the replacement of existing subcontractors. Company shall be entitled to withholding consent only for material reasons related to statutory data protection regulations. (Note: Other reasons to withhold consent to the use of subcontractors will typically be regulated in the Agreement.)

Var. 2
Company hereby consents to Supplier's use of subcontractors. Supplier shall, prior to the use or replacement of subcontractors, inform Company thereof. (If applicable, include notice period or regulation for emergency situations.)

Company shall be entitled to contradict any change notified by Supplier within a reasonable period of time and for materially important reasons. Where Company fails to contradict such change within such period of time, Company shall be deemed to have consented to such change. Where a materially important reason for such contradiction exists, and failing an amicable resolution of this matter by the parties, Company shall be entitled to terminating the Agreement. (This is optional.)

Var. 3
Supplier shall not be entitled to use subcontractors as part of Supplier's performance under the Agreement.

(3) Where Supplier commissions subcontractors, Supplier shall be responsible for ensuring that Supplier's obligations on data protection resulting from the Agreement and this exhibit are valid and binding upon subcontractor.

§ 8 Obligations to inform, mandatory written form, choice of law

(1) Where the Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while in Supplier's control, Supplier shall notify Company of such action without undue delay. Supplier shall, without undue delay, notify to all pertinent parties in such action, that any data affected thereby is in Company's sole property and area of responsibility, that data is at Company's sole disposition, and that Company is the responsible body in the sense of the GDPR.

(2) No modification of this annex and/or any of its components – including, but not limited to, Supplier's representations and warranties, if any – shall be valid and binding unless made in writing or in a machine-readable format (in text form), and furthermore only if such modification expressly states that such modification applies to the regulations of this annex. The foregoing shall also apply to any waiver or modification of this mandatory written form.

(3) In case of any conflict, the data protection regulations of this annex shall take precedence over the regulations of the Agreement. Where individual regulations of this annex are invalid or unenforceable, the validity and enforceability of the other regulations of this annex shall not be affected.

(4) This annex is subject to the laws of [XXX].

§ 9 Liability and damages

Var. 1
Company and Supplier shall be liable to data subject in accordance with Article 82 of the GDPR.

Var. 2
An individual agreement between Company and Supplier which takes into account the specific circumstances and the interests of both parties. (Note: Such an agreement could be as follows: The regulations on the parties' liability contained in the Agreement shall be valid also for the purposes of Contract Processing, unless expressly agreed upon otherwise.)

Where applicable, attach an exhibit on technical and organisational security measures in accordance with Article 32 of the GDPR (see also section 3 para. 2 of this template exhibit)

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.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom