

TEMPLATE · TOMORIS TOOLBOX

Data Processing Agreement (DPA): Template Under Art. 28 GDPR with Review Checklist

Template with twelve sections and four annexes, backed by Art. 28 GDPR, EDPB Guidelines 07/2020 and Implementing Decision (EU) 2021/915

UPDATED

Oct 25, 2026

LENGTH

PDF, 9 pages

ONLINE

tomoris.com/en/downloads/av-vertrag-vorlage

AT A GLANCE

12

Sections of sample text with placeholders

4

Annexes: processing, TOMs, sub-processing, contacts

lit. a–h

Mandatory content under Art. 28(3) GDPR covered

15

Review points for agreements presented to you

WHO IT IS FOR

- Management and purchasing teams that engage service providers with access to personal data
- Those responsible for data protection and data protection officers
- IT service providers, hosting and cloud providers acting as processors
- Legal advisors looking for a starting text for negotiations

WHAT THIS COVERS

If you have a service provider process personal data, Art. 28 GDPR requires an agreement that governs the subject matter, instructions, security, sub-processors, assistance and deletion. This template implements the mandatory content in twelve sections with placeholders, adds the recommendations of the European Data Protection Board from Guidelines 07/2020 and explains when the European Commission's standard contractual clauses are the better choice. The review checklist helps you check an agreement presented by a service provider for gaps in a short time.

TOMORIS template, not an official text: it must be adapted to the specific processing, the main agreement and your company. It provides an overview and does not replace legal advice; the text of the law in its current version is decisive.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01	When you need a data processing agreement	2
02	Mandatory content and where it appears in the template	3
03	Sample text, part 1: subject matter, instructions, security	4
04	Sample text, part 2: assistance, audits, termination	5
05	Annexes to fill in	6
06	Review checklist for a data processing agreement presented to you	7
07	Common mistakes	8
08	Sources	8

01 —

When you need a data processing agreement

The service provider's role, the form of the agreement and the two options: your own agreement or the European Commission's standard contractual clauses.

If a service provider processes personal data on behalf of and according to the instructions of another party, it is a processor. The controller may only use processors that provide sufficient guarantees to implement appropriate technical and organizational measures (Art. 28(1) GDPR). Processing is governed by a contract, which must be in writing, including in electronic form (paras. 3 and 9). According to the European Data Protection Board (EDPB), whether someone is a controller or a processor follows from the factual circumstances and is not negotiable (Guidelines 07/2020, para. 12). If a processor infringes the GDPR by determining the purposes and means of processing itself, it is considered a controller in respect of that processing (Art. 28(10)).

Art. 28(6) to (8) allows an individual contract or standard contractual clauses, in whole or in part; such clauses are laid down by the Commission (para. 7) or a supervisory authority (para. 8).

Your own agreement

The parties negotiate an agreement with all mandatory content, for example based on this template. According to the EDPB, it should not merely restate the GDPR but specify how the obligations will be met and which level of security applies (para. 112).

Standard contractual clauses

The clauses in the Annex to Implementing Decision (EU) 2021/915 meet the requirements of Art. 28(3) and (4) (Art. 1). The parties undertake not to modify them, except to add or update information in the annexes (Clause 2(a)). They may be included in a broader contract and supplemented, as long as nothing contradicts them (Clause 2(b)).

This is a TOMORIS template, not an official text, and it is not identical to the standard contractual clauses. A contract or other legal act is mandatory; whether it is based on the standard contractual clauses or negotiated individually is up to you. The clauses are not necessarily preferable (EDPB, para. 106). Adapt the template to the specific processing and have it reviewed by a lawyer if needed; it does not replace legal advice.

02

Mandatory content and where it appears in the template

What Art. 28(3) GDPR strictly requires, with the section of this template that covers it.

Mandatory content under Art. 28(2) to (4) GDPR and its implementation in the template

MANDATORY CONTENT	REFERENCE	TEMPLATE
Subject matter and duration, nature and purpose, type of data, categories of data subjects, obligations and rights of the controller	Art. 28(3), first sentence	§ 1, § 2, § 9, Annex 1
Processing only on documented instructions, including for third-country transfers; notice in case of an instruction that infringes data protection law	Art. 28(3)(a), second subparagraph	§ 2, § 8
Confidentiality of authorized persons	Art. 28(3)(b)	§ 3
All measures required under Art. 32	Art. 28(3)(c)	§ 4, Annex 2
Conditions for sub-processors: authorization, information, objection, same obligations	Art. 28(2), (3)(d) and (4)	§ 5, Annex 3
Assistance with data subject requests	Art. 28(3)(e)	§ 6
Assistance with security, breach notification, impact assessment, consultation (Art. 32 to 36)	Art. 28(3)(f)	§ 7
Deletion or return at the controller's choice, deletion of existing copies	Art. 28(3)(g)	§ 10
Evidence, audits and inspections	Art. 28(3)(h)	§ 9

03 —

Sample text, part 1: subject matter, instructions, security

§ 1 to § 5 to adopt and adapt; square brackets are placeholders or choices.

Data processing agreement under Art. 28 GDPR between [Name, address] as controller and [Name, address] as processor, hereinafter the parties.

§ 1 Subject matter and duration. (1) The processor processes personal data on behalf of the controller within the scope of [main agreement, MM/DD/YYYY]. The subject matter, nature and purpose of the processing, type of data, categories of data subjects and places of processing are set out in Annex 1. (2) This agreement applies from [MM/DD/YYYY] for the term of the main agreement [or: until MM/DD/YYYY]; obligations under § 10 continue to apply beyond that until they have been fulfilled. (3) The controller provides the data, issues and documents instructions (§ 2) and monitors the processing, including through audits (§ 9).

§ 2 Instructions. (1) The processor processes the data only on documented instructions from the controller, including with regard to transfers to a third country or an international organization, unless required to do so by Union or Member State law; in such a case, the processor informs the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. (2) Instructions are issued in text form by the persons named in Annex 4; the parties keep them together with this agreement. (3) If the processor considers an instruction to infringe data protection law, it informs the controller without undue delay and may suspend its execution until the instruction is confirmed, amended or withdrawn.

§ 3 Confidentiality. The processor grants access to the data only to persons who need it for their tasks and ensures that they have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

§ 4 Security of processing. (1) The processor takes all measures required under Art. 32 GDPR, at a minimum those specifically described in Annex 2. (2) It reviews them regularly, at least [annually], for their appropriateness. (3) Changes that could lower the level of protection require the controller's prior consent in text form; the processor communicates other changes [within deadline].

§ 5 Sub-processors. (1) Choose the applicable option. Option A, specific authorization: the processor engages other processors only with the controller's prior specific authorization in text form and requests it at least [deadline] in advance. Option B, general authorization: the controller authorizes the sub-processors listed in Annex 3. The processor informs the controller in text form at least [deadline] in advance of any intended addition or replacement; the controller may object within [deadline], with the following consequence: [provision]. (2) The processor contractually imposes on each sub-processor the same data protection obligations as set out in this agreement and remains liable to the controller for their fulfillment (Art. 28(4) GDPR).

04 —

Sample text, part 2: assistance, audits, termination

§ 6 to § 12: data subject rights, data breaches, third countries, evidence, deletion, violations and final provisions.

§ 6 Rights of data subjects. The processor forwards requests from data subjects to the controller without undue delay and does not respond to them itself, unless the controller authorizes it to do so. It assists the controller with appropriate technical and organizational measures in responding, for example through [export, rectification, deletion in the system].

§ 7 Assistance with obligations under Art. 32 to 36 GDPR. (1) The processor notifies the controller of every personal data breach without undue delay, no later than [number] hours after becoming aware of it, to [contact from Annex 4], with the information known to it under Art. 33(3) GDPR; it provides missing information as soon as it becomes available. (2) It assists the controller with security measures, notifications to the supervisory authority and data subjects, data protection impact assessments and prior consultation, taking into account the nature of the processing and the information available to it.

§ 8 Places of processing and third countries. Processing takes place at the locations listed in Annex 1. Transfers to a third country or an international organization, including by sub-processors or through remote access, take place only on documented instructions and only if the conditions of Chapter V GDPR are met; basis: [adequacy decision under Art. 45, standard data protection clauses under Art. 46(2)(c) GDPR (Implementing Decision (EU) 2021/914)].

§ 9 Evidence and audits. (1) The processor makes available to the controller all information necessary to demonstrate compliance with this agreement and with Art. 28 GDPR. (2) It allows for and contributes to audits and inspections conducted by the controller or an auditor mandated by the controller; on-site inspections are carried out with [deadline] advance notice. The controller may take into account certifications and audit reports of the processor; the controller selects the auditor. (3) Costs: [provision].

§ 10 Deletion and return. After the end of the services, the processor, at the controller's choice, deletes all personal data and confirms this in text form, or returns it in [format] and deletes existing copies, unless Union or Member State law requires storage. The controller makes the choice [in the agreement: deletion or return] and may change it until the end of the services. This agreement remains in force until deletion.

§ 11 Violations and termination. If the processor cannot comply with this agreement, it informs the controller without undue delay. The controller may then have the processing suspended and terminate the agreement, insofar as it concerns the data processing, if compliance is not restored within [deadline].

§ 12 Final provisions. In the event of conflicts between this agreement and the main agreement, this agreement takes precedence in matters of data protection. Amendments must be made in text form. Text form within the meaning of this agreement is a declaration that can be stored permanently and identifies the person making it, such as an email (electronic form under Art. 28(9) GDPR). Liability is governed by [main agreement]; Art. 82 GDPR remains unaffected. Annexes 1 to 4 form part of this agreement. Place, date, signatures of both parties.

05 —

Annexes to fill in

Description of the processing, technical and organizational measures, sub-processors and contacts.

Annex 1: Description of the processing (Art. 28(3) sentence 1 GDPR)

ITEM	ENTRY
Subject matter: main subject of the processing, precise enough for third parties to understand	_____
Nature and purpose of the processing: operations such as storage, backup, remote maintenance, sending, and for what purpose	_____
Type of personal data, name special categories specifically	_____
Categories of data subjects, e.g. employees, customers, visitors	_____
Duration of the processing or criteria for it	_____
Places of processing, including remote access and support	_____

Annex 2: Technical and organizational measures, described specifically rather than in general terms

AREA UNDER ART. 32(1) GDPR	MEASURES OF THE PROCESSOR
a) Pseudonymization and encryption	_____
b) Confidentiality, integrity, availability and resilience of systems and services	_____
c) Timely restoration after an incident	_____
d) Regular testing and evaluation of effectiveness	_____

Annex 3: Authorized sub-processors

NAME, ADDRESS	SERVICE	LOCATION, BASIS IF THIRD COUNTRY
_____	_____	_____
_____	_____	_____

Annex 4: Persons authorized to give instructions and contacts

ROLE	CONTROLLER	PROCESSOR
Authorized to give instructions or recipient of instructions	_____	_____
Notifications of personal data breaches	_____	_____
Data protection officer, if appointed	_____	_____

06 —

Review checklist for a data processing agreement presented to you

Many service providers present their own agreements; these points show quickly whether anything is missing.

- ☐ The roles match reality: the service provider does not decide on purposes itself, such as its own analyses or training with your data
- ☐ Subject matter, nature, purpose, types of data and data subjects are described specifically, not just "personal data under Art. 4" (EDPB, para. 114)
- ☐ Processing only on documented instructions; it is defined who issues instructions and how they are documented
- ☐ Obligation to notify in case of instructions that infringe data protection law, and the consequence, such as suspension (EDPB, para. 149)
- ☐ Confidentiality commitment of the service provider's employees
- ☐ TOMs described specifically or attached as a current document; changes not at the expense of the level of protection
- ☐ Sub-processors: list provided, specific or general authorization, notice period, right to object and its consequence, same obligations and the service provider's liability for them
- ☐ Places of processing stated, third-country transfers only with a basis under Chapter V
- ☐ Assistance with data subject rights, without the service provider responding to requests itself
- ☐ Notification of personal data breaches without undue delay, with a deadline in hours, a point of contact and minimum information (EDPB, para. 136)
- ☐ Assistance with impact assessments and consultation
- ☐ Evidence and audit rights for you or an auditor mandated by you, not just certificates of the service provider's choosing
- ☐ Deletion or return at your choice, deletion of existing copies, with confirmation and deadline
- ☐ Precedence of the data processing agreement over general terms and conditions in matters of data protection
- ☐ Concluded and filed in writing or electronically, with a reference in the record of processing activities

07 —

Common mistakes

What weakens data processing agreements in practice and how to avoid it.

- The agreement only restates Art. 28: without specific instructions, deadlines and measures, nothing can be proven when it matters (EDPB, para. 112).
- Standard contractual clauses reworded: if you change their text, you are no longer using the clauses whose adequacy the decision establishes (Art. 1); you may only supplement the annexes and add non-conflicting clauses (Clause 2).
- The list of sub-processors is missing or outdated; changes are only published on a website, without giving you the opportunity to object.
- Role misclassified: not every service provider is a processor. Anyone who decides on purposes and essential means themselves is a controller (EDPB, para. 39 f.); in that case, a data processing agreement does not fit, but rather, for example, an arrangement under Art. 26 GDPR for joint controllership.
- Agreement concluded but never put into practice: instructions not documented, audits never carried out, deletion at the end not confirmed.

NEXT STEP

Check It Yourself or Put It into Practice Together

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

08 —

Sources

All statements are supported by sources. Legislation applies in its current version.

- | | |
|--|---|
| <p>1 Regulation (EU) 2016/679 (GDPR), corrigendum OJ L 127 of May 23, 2018
Art. 26, 28, 29, 32, 33(3), 45, 46, 82 and Chapter V; Art. 28(3)(g) in the corrected version
eur-lex.europa.eu/eli/reg/2016/679/oj/deu</p> | <p>2 Implementing Decision (EU) 2021/915: standard contractual clauses under Art. 28(7) GDPR
Art. 1 and 2, Recitals 5 and 6, Clauses 2, 7, 8, 9 and 10, Annexes I to IV
eur-lex.europa.eu/eli/dec_impl/2021/915/oj/deu</p> |
| <p>3 Implementing Decision (EU) 2021/914: standard contractual clauses for third countries
Art. 1(1): safeguards under Art. 46(2)(c) GDPR
eur-lex.europa.eu/eli/dec_impl/2021/914/oj/deu</p> | <p>4 EDPB Guidelines 07/2020 on the concepts of controller and processor
Version 2.0 of July 7, 2021, paras. 12, 39 f., 104 to 159
www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_...</p> |

**5 Digital Omnibus proposal COM(2025) 837, procedure
2025/0360(COD)**

reviewed: no amendment to Art. 28 GDPR proposed; pending as of
October 25, 2026

eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025PC0837