



## Explanatory notes on using the Model Data Processing Agreement (ARIV)

These explanatory notes are in the public domain, but are not part of the Contract. The notes can help resolve any doubts about the meaning and/or interpretation of the Model Data Processing Agreement, which is governed by the General Conditions for Government Purchasing (ARIV). The notes do not affect the actual agreements made by the Parties.

### I – Introduction

When an Contract is awarded on the basis of the ARIV, the Contract may require the Supplier to process Personal Data on behalf of the Purchaser. If so, the Parties must conclude a Data Processing Agreement under article 28, paragraph 3 of the General Data Protection Regulation ('the Regulation'). In a Data Processing Agreement the Purchaser and the Supplier make agreements on the Processing of Personal Data in the context of the Contract. The agreements relate to the protection of Data Subjects' Personal Data.

If Personal Data is processed during the implementation of a public service contract, a Data Processing Agreement should – in principle – be drawn up using the Model Data Processing Agreement (ARIV). The Data Processing Agreement is then attached as a schedule to the Contract.

The model has been drawn up on the basis of article 28 of the Regulation. The articles of the Model Data Processing Agreement have been formulated to match those of the Regulation as much as possible. Where the text of the Regulation has not been followed to the letter, this is due to national legislation or the content of the Contract/ARIV. The Parties are respectively referred to as 'Purchaser' and 'Supplier' in the model, rather than as 'controller' and 'processor'. The recitals explicitly state that the Purchaser qualifies as a controller within the meaning of article 4 (7) of the Regulation and that the Supplier qualifies as a processor within the meaning of article 4 (8) of the Regulation.

The articles in the model form an integrated whole with the articles of the Contract and the ARIV. Subjects that have already been dealt with in the Contract or the ARIV are therefore not dealt with again in the Data Processing Agreement. The Data Processing Agreement must therefore always be concluded in combination with the Contract and the ARIV.

Article 9 of the ARIV 2018 sets out general provisions to ensure that the Processing of Personal Data under the Contract is lawful. This article is too limited however to meet the requirements for data processing agreements set out in article 28, paragraph 3 of the Regulation.

The model is expressly *not* suitable for use in the following situations:

- a. If the Purchaser does not qualify as a controller for the Processing of Personal Data under article 4 (7) of the Regulation.
- b. If general terms and conditions other than the ARIV have been declared to apply to the Contract.
- c. If the Processing of Personal Data does not fall within the scope of the Regulation, but instead falls within the scope of Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
- d. If Personal Data is processed in a country outside the European Union for which the European Commission has not issued an adequacy decision as referred to in article 45, paragraph 3 of the Regulation and none of the derogations from the ban on Processing referred to in article 49 of the Regulation applies, agreements must be made that meet one of the situations set out in article 47, paragraph 2 or 3 of the Regulation in order to qualify as appropriate safeguards.
- e. If the Supplier is part of the same legal person as the Purchaser, in which case the Civil Service Data Processing Agreements model must be used.

This model comprises 11 standard articles that apply to every Data Processing Agreement. Articles 10 and 11 of the model contain several optional provisions that can be used, depending on the situation in question.

The model contains three mandatory schedules. These schedules must be completed in order to comply with the requirements regarding data processing agreements set out in article 28, paragraph 3 of the Regulation.

The subject matter and purpose of the Processing, the type of Personal Data and the categories of Personal Data, Data Subjects and recipients must be set out in Schedule 1. The technical and organisational security measures must be set out in Schedule 2. The agreements on Personal Data Breaches must be set out in Schedule 3.

## **II – Notes on individual articles**

### **Article 1 Definitions**

First and foremost, this article states that all the definitions given in article 1 of the ARIV 2018 also apply to the Data Processing Agreement. This article also defines a number of other terms used in the Data Processing Agreement.

#### *Data Subject*

In the Regulation, this term is not defined. However, article 4 (1) of the Regulation does contain the phrase: ‘any information relating to an identified or identifiable natural person (“data subject”)’. In the Data Processing Agreement, the definition set out in section 1, opening words and (f) of the Personal Data Protection Act is followed. Nevertheless, the aim is for ‘data subject’ to have the same meaning as in the Regulation.

#### *Personal Data Breach*

Here, the definition given in article 4 (12) of the Regulation has been followed. The definition does not distinguish between breaches that do or do not represent a risk (high or otherwise) to the Data Subject’s rights and freedoms. This distinction is only of importance in relation to the Purchaser’s notification requirements, as referred to in articles 33 and 34 of the Regulation.

#### *Personal Data*

Here, the definition given in article 4 (1) of the Regulation has been followed. However, the definition has been amended to reflect the fact that the term only covers data being processed by the Supplier for the Purchaser under the Contract. This therefore excludes Personal Data that the Supplier processes on a legal basis other than the Contract. For instance, data processing activities for which the Supplier is the controller.

#### *Processing*

Here, the definition given in article 4 (2) of the Regulation has been followed.

### **Article 2 Object of this Data Processing Agreement**

Under article 28, paragraph 3 of the Regulation, the Processing of Personal Data by a counterparty must be governed by a Data Processing Agreement. The agreement must in any event set out: the subject matter and the duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects.

In paragraph 1, the description of the subject matter is linked to the description of the services set out in the Contract. The Contract sets out the services provided by the Supplier.

In paragraph 2, reference is made to Schedule 1, which must be used to set out the other aspects, i.e. the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects. The ministerial record of processing activities, as referred to in article 30 of the Regulation, can be used to complete this schedule.

‘Type of Personal Data’ refers to the following types: (1) special categories of personal data, as referred to in article 9 of the Regulation, (2) personal data relating to criminal convictions and

offences, as referred to in article 10 of the Regulation, (3) identification numbers prescribed by law and (4) other personal data.

Under article 28, paragraph 1 of the Regulation, the Purchaser may only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the Regulation and ensure the protection of the rights of the Data Subject. Paragraph 3 requires the Supplier to provide the relevant guarantees. The guarantees alone are not sufficient, however. The Data Processing Agreement must contain agreements on the concrete measures to be taken by the Supplier.

Paragraph 4 extends the guarantees to cover compliance with all applicable legislation relating the Processing of Personal Data. This primarily concerns the Regulation and the Act implementing the Regulation (GDPR), but also any special legislation. The Supplier undertakes, among other things, to keep, where applicable, a record of processing activities, as referred to in article 30, paragraph 2 of the Regulation, to cooperate with the supervisory authority, as referred to in article 31 of the Regulation, and to designate a data protection officer, as referred to in article 37 of the Regulation. The guarantee ensures that the Purchaser can impose contractual consequences if the Supplier does not comply with its statutory obligations.

### **Article 3 Entry into force and duration**

This article regulates the entry into force and duration of the Data Processing Agreement. Under article 28, paragraph 3, opening words of the Regulation, the duration of the Processing must be specified in the Data Processing Agreement.

Paragraph 1 states that the Data Processing Agreement enters into force as soon as it has been signed by both Parties. In practice, the Data Processing Agreement will be signed and enter into force at the same time as the Contract. The Data Processing Agreement must be concluded before the actual Processing of Personal Data begins.

Paragraph 2 states that the Data Processing Agreement terminates after the Supplier has either deleted or returned all Personal Data in accordance with article 10. Article 10 states that once the Contract expires, the Supplier will erase the Personal Data or return it to the Purchaser. The Data Processing Agreement ends only when this has been done. This means that the Data Processing Agreement may remain in force even after the Contract has been terminated, possibly for some time.

Moreover, under article 25 of the ARIV 2018, termination of the Contract and the Data Processing Agreement does not discharge the Supplier from obligations which, by their nature, remain in force thereafter. Such obligations include those relating to liability, confidentiality, disputes and applicable law.

Paragraph 3 states that neither of the Parties may terminate the Data Processing Agreement before the Contract terminates. This provision has been included because the Data Processing Agreement is linked to the Contract and because the Regulation requires the Parties to conclude an agreement governing the Processing of Personal Data.

### **Article 4 Scope of the Supplier's Processing competence**

This article sets out several obligations for the Supplier that are directly derived from the Regulation (and its system).

Under article 29 of the Regulation, the Supplier and any other entity that is acting under the authority of the Purchaser or Supplier and has access to the Personal Data in question carries out Processing exclusively on instructions from the Purchaser, unless required to do so by Union or member state law. Under article 32, paragraph 4 of the Regulation, the Purchaser and Supplier must take steps to ensure that any natural person acting under either's authority who has access to Personal Data does not process it except on instructions from the Supplier, unless required to do so by Union or member state law. In addition, under article 28, paragraph 3, opening words and (a) of the Regulation, a Data Processing Agreement must in any event specify that Personal Data is processed only on the basis of written instructions from the Purchaser, unless the Supplier is required to carry out processing by Union or member state law.

For that reason, paragraph 1 states that the Supplier is not permitted to process Personal Data except on the basis of written instructions from the Purchaser. The only exception is a situation in which the Supplier must do this as a result of a statutory obligation.

If the Supplier believes that the written instructions from the Purchaser contravene the Regulation or other statutory provisions on the protection of personal data, the Supplier will inform the Purchaser accordingly. This obligation is laid down in paragraph 2 and is taken from article 28, paragraph 3, opening words and (h) of the Regulation.

Paragraph 3 states that if the Supplier is legally required to disclose Personal Data, it will inform the Purchaser, if possible prior to the disclosure. This is because article 28, paragraph 3, opening words and (a) of the Regulation requires the Supplier to inform the Purchaser of such a legal requirement, before Processing begins, unless that law prohibits such information on important grounds of public interest.

Under article 4 (7) of the Regulation, it is the Purchaser that determines the purposes and means of the Processing of Personal Data. Under article 28, paragraph 10 of the Regulation, if the Supplier infringes the Regulation by determining the purposes and means of Processing (i.e. does not adhere to paragraph 1), the Supplier will be considered a controller in respect of that Processing. The Data Protection Authority and Data Subjects can directly hold the Supplier to account in this regard. Paragraph 4 of the Data Processing Agreement states that the Supplier has no control over the purposes and means of the Processing of Personal Data.

## **Article 5 Security measures**

This article covers the security measures relating to the Processing of Personal Data.

Article 32 of the Regulation obliges the controller and the processor to take appropriate technical and organisational measures in order to ensure a level of security appropriate to the risk. Furthermore, under article 28, paragraph 3, opening words and (c), the Data Processing Agreement must stipulate that the processor will take all measures required pursuant to article 32. This is regulated in paragraphs 1 and 2.

Paragraph 1 refers to Schedule 2. The standards and measures that the Supplier must adopt to ensure the security of Processing must be specified in this schedule. Reference may be made to documents setting out standards and measures, such as (where relevant) the programme of requirements, the tender or the request for tenders. Examples of measures include: pseudonymising and encrypting Personal Data, monitoring and logging, screening Staff, and physical security measures to prevent unauthorised access.

These measures must guarantee an appropriate level of security, taking account of the latest technology and the costs of implementing such measures. The level of security appropriate in a specific case must be determined on the basis of a risk analysis carried out by the Purchaser. In addition, specific types of service provision may entail specific security requirements. Service provision within the cloud is one example.

It may be the case that not all Personal Data processed by the Supplier is equally sensitive and that the same agreements do not apply to all Personal Data being processed. In such cases, the Data Processing Agreement must lay down which agreements apply to which Personal Data.

Under article 28, paragraph 4 of the Regulation, an approved code of conduct, as referred to in article 40 of the Regulation, or an approved certification mechanism, as referred to in article 42 of the Regulation, can also be adhered to. This is also laid down in article 32, paragraph 3. Examples include the NEN-ISO/IEC 27001 information security standard.

In addition to the Regulation, the Purchaser must also adhere to the following standards frameworks: the 2017 Civil Service Information Security Regulations, the 2013 Civil Service Information Security (Classified Information) Regulations and the 2012 Civil Service Information Security Baseline.

The description of the measures in Schedule 2 is not exhaustive. The description in Schedule 2 does not affect other information security requirements that have already been set, such as those in the programme of requirements. Furthermore, under paragraph 3 and in addition to this

description, the Purchaser can require additional measures to be taken. If, while the Data Processing Agreement is in force, it becomes apparent that the measures agreed upon are insufficient, the Supplier – at the Purchaser's request – must take additional measures to ensure the security of the Personal Data. A reason for taking additional measures might, for instance, be a Personal Data Breach, resulting in the destruction, loss or alteration of the Personal Data.

The words 'without prejudice to article 2.3' in paragraph 1 mean that, aside from the measures included in Schedule 2, the measures taken by the Supplier must always be appropriate within the meaning of article 32 of the Regulation.

Paragraph 3 follows on from this. Whether measures are appropriate depends on external factors and can change while the Data Processing Agreement is in force as a result of technological developments or new risks, for instance. The Parties recognise this. This means that, during the provision of services, they need to check periodically whether the measures taken are appropriate and, where necessary, take additional measures to ensure this remains the case.

Paragraph 4 states that the Supplier may carry out the Processing – including storage – of Personal Data in a country outside the European Union only if it has received express written permission to do so from the Purchaser and barring any statutory obligations to the contrary resting on the Supplier. Under article 28, paragraph 3, opening words and (a) of the Regulation, this provision must be included in a Data Processing Agreement.

If a statutory rule obliges the Supplier to process Personal Data outside the European Union, the Supplier must inform the Purchaser of this statutory rule, unless that law prevents this on important grounds of public interest. This is regulated in article 4.3.

'Outside the European Union' includes Processing by an international organisation. Under article 4 (26) of the Regulation, this means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Articles 44 to 50 of the Regulation lay down conditions for the transfer of Personal Data to third countries and international organisations. The underlying principle is that transfers of this kind must not undermine the level of security guaranteed to natural persons in the European Union by way of the Regulation. Transfer can take place only in full compliance with the Regulation.

If the Parties wish to justify the transfer of Personal Data to a country outside the European Union on the basis of article 46, paragraph 2 or 3 of the Regulation, the Model Data Processing Agreement cannot be used for this purpose. The Purchaser and the Supplier must make specific agreements on providing appropriate safeguards in light of the particular risks of Processing in a country outside the European Union.

Under paragraph 5 the Supplier must inform the Purchaser without unreasonable delay of any illegal or unauthorised Processing of Personal Data or infringements of security measures. It is then the Purchaser's duty to assess whether the relevant parties must be notified of the Personal Data Breach, as set out in articles 33 and 34 of the Regulation.

The Purchaser must have insight into all illegal or unauthorised Processing of Personal Data or infringements of security measures. Under article 33, paragraph 5 of the Regulation, the Purchaser must document all Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken, so that the supervisory authority can verify compliance with articles 33 and 34.

Finally, paragraph 6 states that the Supplier will assist the Purchaser in ensuring compliance with the obligations set out in articles 32 to 36 of the Regulation. Under article 28, paragraph 3, opening words and (f) of the Regulation, this must be set out in the Data Processing Agreement. These articles cover obligations on: taking security measures (article 32), notifying the supervisory authority and Data Subjects of a Personal Data Breach (articles 33 and 34), carrying out a data protection impact assessment (article 35) and prior consultation with the supervisory authority (article 36).

## **Article 6 Duty of Confidentiality of the Supplier's Staff**

Under article 28, paragraph 3, opening words and (b) of the Regulation, the Data Processing Agreement must require the Supplier to ensure that persons authorised to carry out Processing of the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Paragraph 1 states that the Personal Data is confidential, as referred to in article 8 of the ARIV 2018. Under article 8, paragraph 1 of the ARIV 2018, the Supplier may not divulge in any way whatever any information that comes to its attention in the course of performing the Contract and that it know or may reasonably be assumed to know is confidential, except in so far as it is compelled to divulge such information under a statutory regulation or court ruling. In addition, article 8, paragraph 2 of the ARIV 2018 states that the Supplier must impose on its Staff the same duty of confidentiality. Paragraph 4 provides for the imposition of a penalty under the Contract if the Supplier breaches its duty of confidentiality.

Paragraph 2 requires the Supplier to show – at the Purchaser's request – that its Staff have undertaken to observe the duty of confidentiality. This can be done by providing non-disclosure undertakings signed by Staff, for example.

## **Article 7 Subprocessors**

Under article 28, paragraph 2 of the Regulation, the Supplier must not engage another processor without prior specific or general written authorisation of the Purchaser. Under article 28, paragraph 3, opening words and (d) of the Regulation, this authorisation must be agreed in writing.

Under article 28, paragraph 4 of the Regulation, the Supplier must impose the same obligations regarding the protection of Personal Data on the processors it has engaged as those agreed by it and the Purchaser. In addition, that paragraph states that where the other processor fails to fulfil its data protection obligations, the Supplier remains fully liable to the Purchaser for the performance of the other processor's obligations. Under article 28, paragraph 3, opening words and (d) of the Regulation, this must be included in the agreement.

## **Article 8 Assistance concerning rights of Data Subjects**

Under article 28, paragraph 3, opening words and (e) of the Regulation, the Supplier must assist the Purchaser in fulfilling its obligation to respond to requests from Data Subjects to exercise the rights set out in chapter III of the Regulation. This is laid down in article 8.

This article relates to the rights of Data Subjects referred to in articles 12 to 22 of the Regulation. These are the right to information and access to Personal Data, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability and the right to object.

## **Article 9 Personal Data Breach**

In addition to the obligation referred to in article 5.4, paragraph 1 sets out the way in which the Supplier must inform the Purchaser of Personal Data Breaches. Schedule 3 must set out how the Supplier will inform the Purchaser and the minimum information that the Supplier must provide to the Purchaser.

On the basis of this information, the Purchaser must be able to determine whether or not relevant parties need to be notified of the Personal Data Breach, as referred to in articles 33 and 34 of the Regulation. The Purchaser must also be able to comply with its obligation to register all Breaches (article 33, paragraph 5 of the Regulation). This means that article 9 also relates to article 28, paragraph 3, opening words and (f) of the Regulation.

Paragraph 2 states that the Supplier must inform the Purchaser – including after a notification on the basis of paragraph 1 – of developments relating to a Personal Data Breach, so that the Purchaser can comply with its obligations, including those set out in articles 33 and 34 of the Regulation.

Paragraph 3 states that the Parties will bear any costs they incur in notifying the Data Protection Authority of the Personal Data Breach.

### **Article 10 Return or erasure of Personal Data**

This article is connected with article 3, which relates to the duration of the Data Processing Agreement. Under paragraph 2, this Data Processing Agreement terminates only after and in so far as the Supplier has deleted or returned all Personal Data in accordance with article 10. This means that the Data Processing Agreement may remain in force after the Contract has been terminated, possibly for an extended period of time.

Under article 28, paragraph 3, opening words and (g) of the Regulation, the Data Processing Agreement must state that the Supplier, after Processing has been completed, at the choice of the Purchaser, deletes or returns all Personal Data to the Purchaser, and deletes existing copies unless the Supplier is required by law to store the Personal Data. This is regulated in paragraph 1.

Paragraph 2 is an optional provision. It can be used to specify how long the Supplier has to delete or return Personal Data, after the Contract is terminated. The article also states that the Supplier must pay the Purchaser a fine for each day it is in default. The amount per day and the maximum amount must be filled in. The amounts should be proportional.

Paragraph 3 is also an optional provision. The model contains two alternatives. These alternatives relate to cases where Personal Data must be returned to the Purchaser. The first alternative states that the format in which the Personal Data must be returned will be determined by the Purchaser in due course. The second alternative allows the procedure for return to be included in the Data Processing Agreement.

### **Article 11 Obligation to supply information and audit obligation**

The Purchaser must ensure or be able to ensure that the Supplier and any other processors comply with the Data Processing Agreement. Under article 28, paragraph 1 of the Regulation, the Purchaser may engage the Supplier only if the latter provides sufficient guarantees to implement appropriate measures in such a manner that Processing will meet the requirements of the Regulation and ensure the protection of the rights of the Data Subject.

On the basis of article 28, paragraph 3, opening words and (h) of the Regulation, the Data Processing Agreement must state that the Supplier will make available to the Purchaser all information necessary to demonstrate compliance with the obligations laid down in that article and allow for and contribute to audits, including inspections, conducted by the Purchaser or another auditor mandated by the Purchaser. This is laid down in paragraphs 1 and 2.

Paragraph 3 is an optional provision with two alternatives. The first alternative is for a situation in which the Purchaser instructs an independent party to carry out an audit. It must be specified how frequently the Purchaser will do this. The second alternative is for a situation in which the Supplier instructs an independent external expert to carry out an audit. It must be specified how frequently the Supplier will do this and the relevant deadline.

If the audit shows that the security measures taken are not sufficient, the Purchaser can, on the basis of article 5.2, require the Supplier to take additional measures, in order to guarantee an appropriate level of security.

### III – Transposition table

<i>GDPR</i>	<i>Model</i>	<i>ARIV</i>
28.1	2.3, 11	9.1
28.2	7	
28.3	2.1, 2.3, 3, Schedule 1	9.2
28.3.a	4.1, 4.3, 5.3	
28.3.b	6.1	8
28.3.c	5.1, Schedule 2	
28.3.d	7	
28.3.e	8	
28.3.f	5.2, 5.4, 5.5, 9.1, Schedules 2 and 3	
28.3.g	3.2, 10.1	
28.3.h	4.2, 11.1	
28.4	7	
28.10	4.4	

#### **Publication information**

These notes were drawn up under the responsibility of the interministerial Advisory Committee on Corporate Legal Affairs (CBA).

Further information may be obtained from the CBA Secretariat ([cba@minbzk.nl](mailto:cba@minbzk.nl)).

Published May 2018