December 2022

Explanatory notes to the Data Processing Agreement of *Brancheorganisaties Zorg* (Association of Healthcare Sector Organizations)

United in

December 2022

Introduction

In late 2017, ActiZ, De Nederlandse GGZ, NFU, NVZ and VGN, united in the Association of Healthcare Sector Organizations (*Brancheorganisaties Zorg* or BoZ), drafted a model data processing agreement in connection with the entry into force of the General Data Protection Regulation (GDPR). In late 2022 it was high time to update that model agreement. These explanatory notes set out the main principles of the BoZ data processing agreement and outline the important changes that have been made.

To facilitate the provision of proper healthcare, it is necessary for healthcare providers to prepare client records. These therefore contain highly sensitive data. The right to privacy is enshrined in legislation which requires those who process these special categories of personal data to treat the data with the utmost care. For that reason, it is essential to make clear and robust agreements with parties who handle these special categories of personal data on behalf of healthcare providers to ensure that these data are processed securely and responsibly at all times. These agreements with the service provider can (and must) be set forth in a data processing agreement.

Legal obligation

Entering into a data processing agreement is a legal obligation if a healthcare provider engages a third party to process personal data on its behalf, for example a supplier of a client record.

A data processing agreement is concluded between a controller and a processor. A *controller* is the party which – by law, as a result of agreements made or due to circumstances – has responsibility for processing and which determines the purposes and means of processing. In the healthcare sector, the controller is usually the party which has entered into the healthcare agreement with the client and, for that reason, keeps a healthcare record on that client. The controller determines what data are processed and how and why data are processed. A *processor* is the party which processes personal data *exclusively* on behalf and on the instructions of the controller. The processor may not use the personal data for its own purposes.

Controller or processor?

It is not always easy to determine who is a controller and who is a processor in a specific case. The following considerations can help determine this:

The processor may not make independent decisions on the purpose of processing if the processor may act solely under the responsibility of the controller and on the controller's instructions. If a party does make independent decisions about the purposes and means of data processing, it is considered to be the controller of the data in question. In other words, the processor has no control over the personal data.

A party is a processor if its primary task is the processing of personal data on behalf of the controller: the processor's services must be focused on the processing of personal data on the controller's behalf. If the processing of personal data is not the primary task of a party but a consequence of a different form of service provision, the party in question itself is the controller of the data so processed. In other words, the mere fact of receiving instructions from or providing a service to the controller is not sufficient to qualify as a processor. The instructions must be targeted specifically at the processing of personal data. If the supplier has full control over the data – such as in the case of SaaS solutions and independent management of data residing with the controller – this counts as a primary task, as the supplier's instructions are targeted at the data. If the supplier provides remote support under the direction of the controller and thus only has access to the data at the time the controller opens it up for remote support (via a secure VPN

connection), this service is not focused on data processing but on solving the problem technically, and data processing is not the primary task. It is noted that the Main Agreement should include appropriate provisions regarding access to and handling of that data, aimed at processing the data only for remote control purposes. In addition, agreements should be made regarding confidentiality, the exclusion of additional data processing operations, control of logging and monitoring of logging.

Cooperating with another controller?

In healthcare, it also happens that there is joint responsibility for data processing, for example in case of multidisciplinary care or cooperation between a healthcare provider and local authorities. If a healthcare provider has engaged a sub-contractor to provide part of the care, there will also generally be cooperation between two controllers rather than between a controller and a processor.

If there are many cooperating controllers, it can sometimes be advisable to designate a single legal controller, as it will then be clear to everyone who is the primary contact and who (formally) makes the decisions. This is the structure opted for by the National Exchange Point (*landelijk schakelpunt* or LSP, the national secure network for the exchange of medical information), where all healthcare providers are controllers. It is not always necessary to designate a legal controller when a joint controlling responsibility exists. However, where there is joint responsibility under the GDPR it is always necessary to also conclude an agreement setting out the arrangements for the processing of personal data. But as this agreement is of a different nature than the data processing agreement discussed in these explanatory notes, it will not be discussed any further.

Exchange of data between controllers?

Data transfer agreement (DTA)

If an organization processes personal data for its own purposes and shares these data with another organization that uses the personal data for its own purposes, then there are two independent controllers. Each organization must itself define the purposes and means for its own process. So in that case there is no joint processing responsibility within the meaning of the GDPR. It is important, however, that a data transfer agreement is drawn up for this data exchange between two controllers.

The European Data Protection Board (EDPB) has issued guidelines on the concepts of controller and processor in the GDPR. Although the legal form of the arrangement among joint controllers is not specified by the GDPR, the EDPB recommends that such arrangement be made in the form of a *binding* document. One example of such a document is the data transfer agreement.

What is agreed in a data transfer agreement?
Actually, a data processing agreement is not that much different from a data transfer agreement. A data transfer agreement also specifies what personal data are processed and for what purposes they are processed. It also identifies the party responsible for handling questions and/or requests from data subjects and describes how the security measures are designed and implemented. The data transfer agreement is outside the scope of the data processing agreement and therefore outside the scope of these explanatory notes.

The core elements that can in any case be included in the data transfer agreement are:
- term of the agreement
- purpose and basis of data transfer
- obligations of the parties
- confidentiality and non-disclosure
- security
- data breaches
- rights of data subjects
- liability.

December 2022

Amendments incorporated in the new version of the BoZ data processing agreement

BoZ has evaluated experiences with the previous model agreement in order to identify areas for improvement. Some of the texts have been simplified and unnecessary definitions and redundant articles and provisions have been deleted. Some of the amendments are explained below:

Article 4. Security of Personal Data and audit

There are two versions of article 4: one for the processing of medical data and one for the processing of non-medical personal data. The version of article 4 that does not apply should be deleted. Medical data is a special category of personal data, the processing of which requires a higher level of security. The Dutch Data Protection Authority (AP) has stated that appropriate security for personal data means complying with ISO 27001 and, in case of medical data, also with NEN 7510 and, where applicable, with NEN 7512 and NEN 7513.

The GDPR requires processors to be able to demonstrate that they have appropriate security in place. The guiding principle in the BoZ data processing agreement is that the processor can demonstrate this by adding an ISO 27001 certificate and a NEN 7510 certificate to Schedule 2. If no certificate is available, a Third Party Memorandum (TPM) may be added instead. A TPM is a declaration issued by an independent third party who can assess whether a processor operates in accordance with the relevant ISO and NEN standards. It is important for the controller to have a clear understanding of the aspects for which the service has been certified (scope and content) and, if possible, to also receive a report from an independent auditor.

Examples of measures which the processor should take are:

(a) measures to ensure that only authorized staff members have access to personal data for the defined purposes;

(b) measures whereby the processor gives its staff members and sub-processors access to personal data exclusively via named accounts, whereby the use of those accounts is appropriately logged and whereby the relevant accounts only allow the relevant person or legal entity access to personal data where this is necessary;

(c) measures to protect personal data against accidental or unlawful destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure;

(d) measures to identify vulnerabilities with respect to the processing of personal data in the systems that are used to provide services to the controller;

(e) measures to ensure the timely availability of personal data;

(f) measures to ensure that personal data are processed logically separate from the personal data it processes for itself or on behalf of third parties.

Article 7. Use of sub-processors

It has been decided to replace the prior written consent for each new sub-processor with a notification requirement under which the processor is obliged to notify the controller of the engagement of new sub-processors and the controller may object thereto. As a result, the processor does not have to seek consent from the controller for each new sub-processor. If the controller objects to the new sub-processor, the parties will consult with each other to determine how the objection can be removed or how the agreed services can still be provided. It should be noted that the controller’s permission is

required for any processing operations outside the EEA, also for processing by sub-processors.

Article 8. Liability

In this model data processing agreement is no liability clause admitted to deal specifically with the privacy risks associated with data processing and therefore differed from the liability clauses that are generally included in the main agreement. The liability provisions and the limitations on liability in the main agreement often relate only to the contract value. When the contract value is low, those provisions and limitations are disproportionate to the privacy risks associated with data processing. On the other hand, unlimited liability for the processor is neither acceptable nor insurable.

In connection with potentially high risks for the controller, the following additional provisions, specifically addressing liability for penalties imposed by the Dutch Data Protection Authority, may be included in the main agreement:

- The processor is liable for any loss or damage suffered by the controller, in any event including (without limitation) fines and/or periodic penalty payments (*dwangsommen*) imposed by the Dutch Data Protection Authority or other competent authorities, and claims by data subjects on account of failure by the processor to comply with any of the provisions of this data processing agreement and/or violation of the GDPR.
- The processor indemnifies the controller from and against any financial and other loss or damage suffered by the controller as a result thereof, unless the processor demonstrates that the processor is not liable for such loss or damage and such costs.

Article 9. Term of agreement and termination

Article 9.5 states that additional agreements can be made to mitigate continuity risks in the event of incidents and crisis situations, such as bankruptcy. Examples of such additional agreements are:

(a) agreements about the transfer, at regular intervals, of the data processed by the processor to the controller or to a third party; and/or

(b) agreements about the conclusion of an agreement with a third party under which the third party in question assumes joint and several liability for or guarantees the performance of the agreement; and/or

(c) agreements about the conclusion of a tripartite agreement with a third party under which the third party in question has access, at all times, to all the data and information necessary to be able to perform all or part of the services to be performed under the agreement, if necessary, whether or not under a new agreement, in stead of or in parallel with the processor.

Schedules:

- Schedule 1 has been expanded to include a list for the sub-processors.
- Schedule 2 now clarifies how the processor can prove that it complies with the requirements of the GDPR regarding the security of personal data. The guiding principle is that the processor should attach copies of the ISO 27001 certificate and, where applicable, the NEN 7510 certificate. If the processor does not hold this certification, a declaration by an independent third party may be required. It is recommended not to settle for less, but this is, of course, for the controller to decide. If the above is not an option, it may be provided that the minimum requirements set out above in the explanatory notes to article 4 apply.
- The contact details of the parties' relevant contacts – usually their data protection officers – should be provided in Schedule 3.

- Schedule 4 has been deleted altogether because BoZ wants to promote the use of a uniform model agreement. Of course, it remains possible to agree on departures from the model agreement and to set these out in a Schedule 4 to the data processing agreement.

Guiding principles of the BoZ data processing agreement

The BoZ data processing agreement is based on the following principles:

i. The BoZ data processing agreement serves as a standard for the entire healthcare sector. Use of the data processing agreement requires expertise and legal know-how. If desired, the agreement may be deviated from within the limits of the GDPR. In the event of deviations from the model agreement, it is advisable to seek legal advice about the consequences of such deviations. It is also advisable to leave the text of the model agreement unchanged and to set forth any deviations – including the reasons – in article 4 of the BoZ data processing agreement.

ii. The BoZ data processing agreement forms an integral part of the agreement for services concluded between the parties. The BoZ data processing agreement only regulates the relationship between the controller and the processor with respect to the processing of personal data.

iii. The BoZ data processing agreement may literally become part of the agreement for services. In that case, only one document is created and no misalignment problems arise. The BoZ data processing agreement may also be used as a separate document *in addition to* the agreement for services. To avoid any misalignment in that case, the data processing agreement contains a provision giving precedence to the provisions of the data processing agreement over those of the agreement for services.

iv. No attempt has been made to reproduce the law in the BoZ data processing agreement. Accordingly, matters already provided for by law are not repeated in the BoZ data processing agreement. All articles relating to laws and regulations are confined to the processing of personal data.

v. It is essential to properly describe what personal data may be processed by a processor in the context of the services and how they may be processed, in order to delineate the processor's personal data processing activities. A clear definition of these aspects, coupled with the other provisions of the data processing agreement, means that the controller maintains optimum control over the process. This is particularly essential in healthcare, where sensitive personal data are often processed. This is therefore an important part of the data processing agreement. As the way in which the processor's personal data processing activities are delineated differs from case to case, it is not possible to elaborate on this in these explanatory notes.

vi. The main agreement, usually an agreement for the provision of specific services to a healthcare provider, sets out all other arrangements between the commissioning party (the healthcare provider) and the service provider (the supplier) with respect to the provision by the supplier of services that require the processing of medical and other personal data. An example is an agreement for services under which the supplier provides an application that processes patient data or staff member data, often in the form of software as a service (SaaS) and/or a hosting service and/or technical management. The agreement for services therefore provides for matters such as the cost of providing the service, the technical requirements for providing the service, the SLA provisions, the communication arrangements in the "Document Agreements and Procedures" (DAP), liability in the event that the supplier fails to fulfil its obligations in full, on time or at all, any limitations of that liability, etc.

vii. The data processing agreement has been drafted on the basis of current interpretations of the GDPR. If modifications are necessary as a result of amended legislation, evaluations and/or responses from the field, this version will be updated.