Privacy policy De Regenboog Groep 2018

These regulations apply within De Regenboog Groep in Amsterdam to the processing of data of participants, visitors or clients who are involved The Rainbow Group use facilities and / or services.

These regulations apply to both the hardcopy and electronic processing of data.

1. Definitions

Authority for Personal Data (AP): the supervisory authority, the independent body that ensures that personal data are processed carefully and safely and, if necessary, can impose sanctions if this is not done correctly.

File: any structured personal data that is accessible according to certain criteria.

Person concerned: the person to whom the personal data relates, usually the client, or his (legal) representative.

Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or membership of a trade union, and genetic data, biometric data for the unique identification of a person, or data on health, or data related to a person's sexual behavior or sexual orientation.

Third parties: any person or authority that is not a data subject, controller, processor, or person authorized to process personal data under the direct authority of the controller or the processor.

Data Protection Officer (DPO): official who must or can be appointed by the healthcare provider to inform, advise and supervise the application and compliance with the GDPR and other data protection provisions.

Health data: data on the physical or mental health of a person, including data on health services provided with information about his or her state of health;

Infringement in connection with personal data: a breach of security that inadvertently or unlawfully leads to the destruction, loss, modification or unauthorized disclosure of or unauthorized access to transmitted, stored or otherwise processed data. A 'data breach' therefore includes not only the release (leakage) of data, but also unlawful processing of data.

Personal data: all information about an identified or identifiable natural person ("the person concerned"); an identifiable natural person who can be identified directly or indirectly, in particular by means of an identifier such as a name, an identification number, location data, an online identifier or one or more elements characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

Pseudonymisation: the processing of personal data in such a way that the personal data can no longer be linked to a specific persons concerned without the use of additional data, provided that these additional data are stored separately and technical and organizational measures are taken to ensure that the personal data are not to an identified or identifiable natural person.

Consent of the person concerned: by the person concerned, on the basis of sound, specific, freely and unambiguously given consent in which the person concerned accepts the processing of his or her personal data. This can be done by means of a written or oral statement or an unambiguous active action (such as electronically checking a box).

Processor: the person who processes personal data on behalf of and for the controller (for example an external hosting company, saas supplier, quality auditor or an external payroll administration office).

Processing of personal data: all actions relating to personal data, including in any case collecting, recording, organizing, storing, updating, modifying, retrieving, consulting, using, providing by means of forwarding, dissemination or making available in another form, bringing together interrelations, as well as the protection, erasure or destruction of data.

Responsible for processing: the person who, alone or together with others, determines the purpose of and the means for the processing of personal data; usually the manager of the healthcare provider.

Healthcare provider: De Regenboog Groep

2. Processing of personal data of clients in accordance with the GDPR

2.1 Principles on personal data processing[1]

The healthcare provider is responsible for compliance with the following principles when processing personal data and must be able to demonstrate compliance with these principles ("accountability").[2]

Personal data are only processed within De Regenboog Groep:

- in a manner that is lawful, proper and transparent with regard to the person concerned;
- for specified, explicit and legitimate purposes and may then not be further processed in a way incompatible with those purposes; further processing for purposes of archiving in the public interest, scientific or historical research or statistical purposes[3] is not considered incompatible with the original purposes ("purpose limitation");
- insofar as they are adequate, relevant and limited to what is necessary for the purposes for which they are processed ("minimum data processing" also called "data minimization");
- When the personal details are correct and updated if necessary. All reasonable measures must be taken to ensure that the personal data which are inaccurate in relation to the purposes for which they are processed are erased or rectified without delay ("correctness").
- and kept in a form that makes it possible to only identify the persons concerned in for the purposes for which the personal data is processed and not longer than that; personal data may be stored for a longer period of time in so far as the personal data are processed solely for purposes of archiving in the public interest, scientific or historical research or statistical purposes,[4] provided that the appropriate technical and organizational measures required by this Regulation are taken, in order to safeguard the rights and freedoms of to protect the persons concerned ("storage restriction");
- by taking appropriate technical or organizational measures in such a way that they are adequately protected, and that they are protected against unauthorized or unlawful processing and against unintentional loss, destruction or damage ("integrity and confidentiality").

2.2 Legality of processing[5]

Processing is only lawful if and to the extent that at least one of the following conditions, i.e. the legal basis for processing, is met:

- the person concerned has given permission for the processing of his personal data for one or more specific purposes; the healthcare provider must be able to demonstrate the consent[6] and the persons concerned have the right to withdraw the consent at any time;
- the data processing is necessary for the execution of an agreement to which the person concerned is party to, for example the treatment agreement;
- data processing is necessary to comply with a legal obligation, for example the duty to file in the WGBO (Wet op de geneeskundige behandelingsovereenkomst) or data

[1] Please note: the GDPR regulates the lawfulness of the processing of personal data in article 6. However, this article is after the article on the principles of processing (such as purpose limitation, correctness, etc.). However, if there is no basis for lawful data processing, it is not allowed to be processed at all and thus does not comply with the principles that must be observed when processing personal data.
[2] The principles of processing the processing of personal data and accountability follow from article 5 GDPR
[3] Corresponding article 89, first article, GDPR
[4] Corresponding article 89, first article, GDPR
[5] Article 6 GDPR.
[6] For the conditions attached to the permission, see definitions. As far as juveniles are concerned, the age regimes of the WGbo and Youth Act apply with regard to consent.

provision in case of compulsory admission and forced treatment under the Bopz Act (Wet bijzondere opnemingen psychiatrische ziekenhuizen);
- the data processing is necessary to protect the vital interests of the data subject or another natural person; [7]
- the processing of data is necessary for the proper fulfillment of a task that serves the general interest, which is laid down elsewhere in a law with any further stipulations;
- the data processing is necessary for the representation of the legitimate interests [8] of the controller or of a third party and the interests, fundamental rights or fundamental freedoms of the party whose data is processed do not prevail.

2.3 Conditions for the processing of health data[9]

Health data is one of the categories of special personal data. It is prohibited in the GDPR to process special categories of personal data, unless one of the following conditions [10] is met:

- If the processing is necessary for the purposes of preventive or occupational medicine, for assessing employee fitness, medical diagnoses, providing health care or social services or treatments, or managing health care systems and services or social systems and services, to the extent permitted by national legislation.
- For example, health data may be processed for the purpose of providing health care, under the responsibility of a professional who is bound by professional secrecy or by another person who has been kept confidential under the law or agreement.

Please note: in addition to the lifting of the prohibition to process special health data as mentioned above, a processing basis must also be present to process such data (see also 3.2.2).[11]

2.4 Data processing by the processor

- The healthcare provider may outsource the processing (externally) to a processor and then submit the obligations from the GDPR to the processor in a processor agreement.[12] The healthcare provider only relies on processors who provide adequate guarantees with regard to the application of appropriate technical and organizational measures to ensure that the processing complies with the requirements of this Regulation and that the protection of the rights of the person concerned is guaranteed.[13]
- Processing by a processor is regulated in a (processing) agreement that binds the processor with regard to the healthcare provider and in which the subject, the duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of persons concerned and the rights and obligations of the

[7] The GDPR indicates in recital (46) that the processing of personal data is also considered legitimate if it is necessary for the protection essential for the life of the person concerned or that of another person. This ground for processing is only permitted if the processing cannot obviously be based on another legal basis.
[8] In recitals (47) and (49) of the GDPR: a legitimate interest may be present when there is a relevant and appropriate relationship between the person concerned and the controller, in situations where the data subject is a customer or is employed by the controller. In any case, a careful assessment is required to determine whether there is a legitimate interest. In particular, the interests and fundamental rights of the persons concerned may be more important when personal data are processed in circumstances in which the persons concerned reasonably expect no further processing. The processing of personal data insofar as it is strictly necessary and proportionate with regard to network and information security constitutes a legitimate interest of the controller in question.
[9] Arcticle 9, second paragraph, GDPR.
[10] Article 9 GDPR.
[11] Under the GDPR, Member States are allowed to maintain or introduce other conditions, including restrictions, on the processing of healthcare data (recital (53) GDPR). Consideration can be given to the provisions in the WGBO with regard to professional secrecy. Such provisions will then apply in addition to the provisions of the GDPR. This means that a healthcare provider may only pass data on a person's health to third parties if this is permitted under the GDPR (including the aforementioned conditions) and if there is a ground to break the medical professional secret.
[12] Article 28 GDPR.
[13] For the selection of Suppliers that comply with the GDPR, a checklist will be drawn up that will become available via the website of GGZ Nederland.

healthcare provider are described. Such an agreement must meet the requirements set by the GDPR.[14] GGZ Nederland (Mental Health Netherlands) has developed such a model processor agreement[15] in the BOZ context (branch organization care).

- The processor and anyone who acts under the authority of the healthcare provider or the processor and has access to personal data shall only process these on behalf of the healthcare provider, unless he is obliged to do so by law or regulation.[16]

2.5 Liability of controller and / or processor

1. The healthcare provider (controller) is responsible and liable for damage resulting from the attributable failure or insufficient compliance of the GDPR, including the compliance with the security requirements.[17]
2. The processor, to which the care provider has outsourced (part of) data processing, can also be independently liable for damage or a part of the damage resulting from his or her activities. How that liability is divided is assessed by the non-life insurer or the court. It is important that the healthcare provider makes good agreements with the processor and records this in a processor agreement.[18]

2.6 When may special data other than the health data be processed?

Other special data, for example data relating to race / ethnicity or religion / philosophy of life, may only be processed as a supplement to health data if this is necessary for the proper treatment or care of the person concerned and therefore not systematically with each client. For example, for the use of an interpreter / translator if that is necessary for the explanation of the treatment to the client.

2.7 Confidentiality and provision to third parties

1. Personal data obtained whilst practicing their profession in the (mental) health care are covered by the confidentiality obligation of the care provider. This duty of confidentiality is laid down, inter alia, in the WGBO and / or Youth Act (Jeugdwet) and the BIG Act (wet BIG) and in various professional codes.
2. When providing information to third parties, the law is complied with and the guidelines of GGZ Nederland serve as support. Guides that can be helpful in this: Wegwijzer Professional secrecy in collaborations and Guide for professional secrecy.

2.8 When can data be provided to other parties for scientific research and statistics in the field of public health?

Data processing for purposes of archiving in the public interest, scientific or historical research or statistical purposes shall be subject to appropriate safeguards in accordance with the GDPR for the rights and freedoms of the persons concerned. The safeguards ensure that technical and organizational measures have been taken to ensure compliance with the minimum data processing principle. These measures may include pseudonymisation, provided that such purposes can be achieved. If those objectives can be achieved by further processing that does not or no longer permit the identification of the persons concerned, they must be achieved in this way.[19] There may also be derogations in national law from certain rights of the persons concerned from the GDPR to the extent that these rights threaten to threaten or seriously threaten the achievement of the specific objectives, and such deviations are necessary to achieve those objectives.

The WGBO[20] gives the following deviating provisions for scientific research in the area of

[14] In Article 28, third paragraph, GDPR requirements are set for the processor agreement. For example, sub a indicates that personal data may only be processed on the basis of w ritten instructions from the controller.
[15] An introduction and explanatory notes are also available w ith the model processor agreement.
[16] Artikel 29 GDPR.
[17] See the explanation for the model processor agreement (BOZ).
[18] Model processor agreement, introduction and explanation (BOZ).
[19] Article 89 GDPR.
[20] Article 7:457 and 7:458 BW (Wgbo).

health care. The basic principle is that permission from the client is required for the provision of non-anonymised[21] data. Contrary to this principle, without the client's permission for statistical or scientific research in the field of public health, other information requested about the client or access to the documents may be provided if:

1. the asking for permission is not reasonably possible[22] and when the research is carried out there are such guarantees that the privacy of the client is not disproportionately harmed, or
2. the request for permission, given the nature and purpose of the investigation, cannot reasonably be required and the care provider ensures that data are provided in such a form that it is reasonably possible to avoid redirection to individual natural persons.

Furthermore:

(a) the research serves a public interest;
(b) it has been demonstrated that the research cannot be carried out without the data; and
(c) the client concerned has not expressly objected to the provision of data.

It is important to realize that the above conditions work cumulatively; provision is only possible if all conditions are met.

2.9 Agreements with the researcher

The care provider (controller) and the researcher make written agreements about the measures that the researcher takes to protect the privacy of those involved.

2.10 Storage of personal data

The healthcare provider must keep the hardcopy and electronic personal data in a safe manner, which is in accordance with the applicable laws and regulations. Personal data are not kept longer than is necessary to achieve the purposes for which the data are processed, unless the data are anonymised or if it is necessary for the exercise of the right to freedom of expression and information, for the fulfillment of a legal obligation for the performance of a task in the public interest or in the exercise of official authority conferred on the controller for reasons of public interest in the field of public health for the purpose of archiving in the public interest, scientific or historical research or statistical purposes or for establishing, exercising or substantiating a legal claim.[23]

The healthcare provider determines how long the recorded / registered personal data are retained in accordance with applicable laws and regulations. If no specific term can be mentioned yet: the criteria for determining the retention period.
For health data processed within the care relationship, such as the client's file, different retention periods apply.

For an overview of the applicable storage periods, see the Note storage periods for GGZ Nederland.

3. Rights of the data subjects

3.1 Conditions relating to the implementation of the rights of the data subjects

1. The provision of the information referred to in this section (3.1), the provision of communication and the taking of the measures shall take place free of charge. If the request is manifestly unfounded or excessive, in particular because of its repetitive

[21] Pseudonymisation is a security measure (encryption or separate storage of identifying data separate from the content) that makes it impossible to direct a natural person, but indirect redirection (for example by linking to other already known data) remains possible. Therefore, pseudonymised data remain personal data and the GDPR provisions and those of the sector-specific laws on privacy remain applicable. See also consideration (29) GDPR.
[22] For example, when it concerns a historical investigation into data collected years ago about persons whose addresses can no longer be traced. Parliamentary documents II, 21561, 20, p. 3.
[23] Article 17, third paragraph, GDPR (recital 65).

nature, the healthcare provider may:

a. charge a reasonable fee in the light of the administrative costs involved in providing the requested information or communication and taking the requested measures; or
b. refuse to comply with the request.

It is up to the care provider to prove the manifestly unfounded or excessive nature of the request. [24]

2. The care provider shall provide the person concerned with information about the follow-up given to the request without delay and in any event within one month of receipt of the request. Depending on the complexity of the request and the number of requests, this period can be extended by a further two months if necessary. The healthcare provider notifies the person concerned of such an extension within one month after receiving the request. If the persons concerned submits his or her request electronically, the information will be provided electronically, if possible, unless the data subject requests otherwise.
3. The person concerned can submit requests in writing to the board via info@deregenboog.org

3.2 Information to be provided[25]

1. If the healthcare provider requests data from the persons concerned themselves to process, they informs the persons concerned in a concise, transparent, comprehensible and easily accessible form, [26] prior to obtaining their personal data, about:
   a. the identity and contact details of the healthcare provider;
   b. where applicable, the contact details of the data protection officer
   c. the processing purposes for which the data are intended, as well as the legal basis for the processing;
   d. where applicable, the recipients or categories of recipients of the personal data.
2. In addition, the following additional information must be provided to ensure proper and transparent processing:
   a. the period during which the personal data will be stored or, if this is not possible, the criteria for determining that period;
   b. the options the data subject has to request a request for inspection, rectification or erasure of the personal data or restriction of the processing concerning him, as well as the right to object to the processing and the right to data portability;
   c. If the data processing is based on consent, the data subject must be informed of the right to revoke this consent at any time, without this affecting the lawfulness of the processing on the basis of the permission to withdraw it.
3. If the healthcare provider intends to further process the personal data for a purpose other than that for which the personal data has been collected, the healthcare provider will provide the persons concerned with information about that other purpose and all relevant further information as referred to in the second paragraph of this manual before that processing provision.
4. Paragraphs 1, 2 and 3 of this article shall not apply if and insofar as the persons

[24] Article 12 GDPR.
[25] Please note: the WGBO also has an obligation to provide information on treatment-related matters in Section 7: 448 of the Netherlands Civil Code.
[26] And in clear and simple language. See Article 12, first paragraph, GDPR.

concerned already has the information.

3.3 Information to be provided when the personal data have not been obtained from the data subject[27]

1. If personal data have not been obtained from the persons concerned, the healthcare provider will provide the persons concerned with all information in accordance with the above stated (Article 3.2) under paragraphs 1 and 2 and, moreover, the relevant categories of personal data as well as the source from which the personal data originate.
2. The healthcare provider provides the information referred to in the first paragraph of this article:
    a. within a reasonable period, but no later than one month after the acquisition of the personal data, depending on the actual circumstances in which the personal data are processed;
    b. if the personal data will be used for communication with the persons concerned, at the latest at the time of the first contact with the persons concerned; or
    c. where provision of the data to another recipient is envisaged, at the latest at the time when the personal data are provided for the first time.
    d. If the healthcare provider intends to further process the personal data for a purpose other than that for which the personal data have been obtained, the healthcare provider will provide the data subject with information about that other purpose and all relevant further information as referred to in the first paragraph before that further processing of this article.
3. The care provider does not have to inform the person concerned about the aforementioned information if:
    a. the persons concerned already has the information;
    b. informing the person concerned is impossible or requires a disproportionate effort. In particular for processing for purposes of archiving in the public interest, scientific or historical research or statistical purposes, subject to the conditions and safeguards referred to in Article 89 (1), or to the extent that the obligation referred to in paragraph 1 of this Article realization of the purposes of that processing or threatened with serious jeopardy. In such cases, the healthcare provider shall take appropriate measures to protect the rights, freedoms and legitimate interests of the data subject, including disclosure of the information;
    c. the obtaining or providing of information (as mentioned above) on the basis of legislation and regulations is mandatory for the healthcare provider and that legislation and regulations provide for appropriate measures to protect the legitimate interests of the persons concerned; or
    d. the personal data must remain confidential on account of professional secrecy in the context of legislation and regulations, including a statutory duty of confidentiality.

3.4 Access and copy[28]

1. A person of twelve years of age or older has the right to inspect and receive a copy of the processed data relating to his person. The inspection or copy of the information is provided in so far as the personal privacy of another person is not harmed. For example: information about or provided by third parties (non-professionals), such as family and close relatives or bystanders, is not provided without prior permission from that third party.

[27] Article 14 GDPR.
[28] Article 7:456, 7:457 BW (Wgbo).

2. A legal representative of young people under the age of 16 or of an incapacitated adult is entitled to inspect or copy the file with the same exception for information about or provided by third parties (the other parent, family, close relatives and bystanders) insofar as of these representatives consent to the treatment is required.[29] The representative receives only the information that is necessary for the performance of his duties as a representative.
3. If the counselor cannot be expected to take care of a good counselor by providing information about the client or by providing a copy or a copy of the documents to the (legal) representative, he will not do so.[30] For example, if a minor objects to the provision of (certain) information to the parents or a suspicion of child abuse. In that case, a parent can be refused access to the minor's file. Under certain circumstances, the care provider can in fact be prevented from informing the legal representatives sufficiently to obtain their consent to the treatment of the minor.
4. If the healthcare provider is of the opinion that the requested inspection and / or copies must be provided, this must be done as soon as possible, but no later than within one month. Depending on the complexity of the request / requests and the number of requests, this period may be extended by a further two months if necessary. The healthcare provider notifies the person concerned of such an extension within one month after receiving the request. If the data subject submits his request electronically, the information will be provided electronically, if possible, unless the data subject requests otherwise.[31]
5. The person concerned can submit requests in writing to the board via info@deregenboog.org

3.5 Corrigendum (correction) or addition of personal data and limitation of the processing of personal data[32]

1. The data subject may ask the healthcare provider to rectify (correct) his or her personal data if this is incorrect or if the healthcare provider requests the completion of his / her personal data, with due regard for the purpose of the processing, including through his own supplementary to add a statement to his file.
2. The care provider shall inform the applicant without delay and at the latest within one month of receiving a request for supplementation, rectification or erasure (deletion) of data whether and how the request is being complied with.[33] The healthcare provider has the option to extend the one-month term by another two months depending on the complexity of the request. In that case, the person concerned must be informed of this extension within one month.
3. If the healthcare provider rejects the request of the person concerned, he gives the reason for this in writing. The healthcare provider informs the applicant of the rejection of the request without delay and at the latest within one month of receipt of the request. The healthcare provider also informs the applicant about the possibility of submitting a complaint to the Dutch Data Protection Authority and the possibility to lodge an appeal with the court.
4. The persons concerned may ask the healthcare provider to foreclose certain data for certain persons and to have them block access to these data.
5. The request from a client and the decision of the healthcare provider to rectify (correct), erase or add data will be retained in the client's file.

[29] In the WGBO, the minority limit is reduced from 18 to 16 years. In the case of young people who have reached the age of 16, permission from the parents (legal representatives) and the provision of the necessary information to give permission is therefore not necessary, unless the person concerned is unable to do so.
[30] Section 7: 457, third paragraph, of the Dutch Civil Code (Wgbo).
[31] Article 12 GDPR (general rules for exercising the rights of the person concerned).
[32] Article 12 GDPR e.v. GDPR, article 16 GDPR.
[33] The person concerned must provide the information in writing or by other means, including, where appropriate, electronic means.

3.6 Right to data change (forgetfulness)[34]

1. The person concerned has the right to obtain from the care provider uninsured personal data about himself or herself without any unreasonable delay and the healthcare provider is obliged to delete personal data without unreasonable delay if one of the following applies:

(a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws the authorization on which the processing is based and there is no other legal basis for the processing;

c) the personal data have been processed unlawfully;

d) the personal data must be deleted on the basis of a statutory obligation that applies to the healthcare provider.

2. The person concerned can submit requests in writing to the board via info@deregenboog.org

3. The healthcare provider notifies each recipient to whom personal data have been provided of the erasure (deletion) of personal data, unless this proves impossible or requires a disproportionate effort. The healthcare provider will provide the data subject with information about these recipients if requested by the data subject.[35]

4. When the healthcare provider has disclosed the personal data and is required to delete the personal data in accordance with paragraph 1, it shall take reasonable measures, taking into account available technology and implementation costs, and including technical measures, to inform data controllers processing personal data that the person concerned has requested the data controllers to delete any link to, or copy or reproduction of that personal data.

6. If it concerns health data, the healthcare provider will delete the data without unreasonable delay and in any case will provide the data subject within one month of receiving the request information a follow-up to the request. Depending on the complexity of the requests and on the number of requests, this period may be extended by a further two months, if necessary. The healthcare provider informs the person concerned of such an extension within one month of the receipt of the request.

7. A request for data exchange may only be refused if:

(a) the law opposes the destruction;

For example: the file created within a compulsory treatment must be kept five years after the end of the BOPZ treatment or stay in the hospital. A request for cancellation from a client within five years cannot be honored;

b) a third party has a substantial interest in the storage of that data.

For example: a child of a client has a hereditary disease;

c) the client has filed a procedure against the counselor or it is likely that he will do so;

d) the data contains data about (suspected) child abuse, this data can only be destroyed at the request of the child on the basis of the Domestic Violence and Child Abuse Reporting Code and it can only be considered if the child has reached the age of 16 and is competent to do so.

e) the healthcare provider needs the data for the institution exercise or substantiation of a legal claim;

f) for reasons of public interest in the field of public health.

8. The request for erasure of health data and the response thereto shall be retained by the healthcare provider.[36]

---

[34] Article 17 GDPR in conjunction with article 12 paragraph 3 GDPR.

[35] Article 19 GDPR.

[36] In that case, a physical proof can be shown to the financier that the file has been destroyed at the request of the person concerned.

3.7 Righ of objection[37]

1. The person concerned has the right to object at any time, for reasons related to his specific situation, to the processing of personal data concerning him or her on the basis of the necessity for the fulfillment of a general interest, or of a task in the exercise of the public authority that is entrusted to the healthcare provider, or on the basis of the necessity to look after the legitimate interests of the care provider or of a third party;
2. The healthcare provider will assess without delay, and in any case within one month after receiving the objection, whether the objection is justified. If the objection is justified, it immediately will terminate the processing, unless there are compelling legitimate reasons for the processing that outweigh the interests, freedoms and rights of the person concerned, or that are connected with the institution's exercise or substantiation of a legal claim.

3.7 Right to data portability (data portability) [38]

1. The person concerned has the right to obtain the personal data concerning him or her which he or she has provided to a healthcare provider in a structured, current and machine-readable form, and he or she has the right to transfer this data to another controller (for example, another healthcare provider) without be prevented from doing so by the care provider to whom the personal data had been provided, in case the processing is based on permission or on execution of an agreement, and the processing is carried out automatically.
2. In exercising the right to data transferability, the person concern has the right to transfer the personal data, if technically possible, directly from one healthcare provider to another.
3. In exercising this right, this may not affect the rights and freedoms of others.

3.9 Representation

1. In the case of a child under the age of twelve and in the case of an incapacitated young person between the ages of 12 and 18, the parent(s) with authority or the guardian shall exercise the rights of the young person, unless this is not compatible with the care of the child from a good social worker.[39]
2. The parent who has no authority will receive important, general and factual information[40] on the health status of the young person on request, unless:
    a) the care provider has not provided or provided the information to the parent with authority;
    b. not compatible with the care of a good care provider.
3. The adolescent of twelve years or older willingly and independently exercises his or her rights regarding his or her personal and health data. The destruction of data regarding (suspicion of) child abuse will only take place with the permission of a willing adolescent of sixteen years and older.
4. If the person concerned is older than eighteen years of age, and incapable of dealing with the matter, then it will act on his or he behalf:
    a) a (assigned) curator or mentor;
    b) if there is no curator or mentor, the person whom the client has authorized in writing;
    c) in case the person's representative is absent or does perform as such, the spouse or partner of the person concerned;
    d) in case the spouse or partner is missing or does perform as such, a child, brother or sister of the person concerned.

5. In the extreme case, the care provider will act as a good care provider; it will ensure that a legal representative for the person involved takes action as quickly as possible. If necessary,

[37] Article 21 GDPR.
[38] Article 20 GDPR.
[39] Article 457 of the Dutch Civil Code (Wgbo), This may be the case if the care provider believes that it is not in the interest of the child or if the young person does not want certain information to be provided.
[40] Only information that is factual, global, important and purposeful can be provided.

if family or neighbor is unable or unwilling to do so, he requests the judge to appoint a representative.

4. Secure processing of personal data

4.1 Responsibility of the controller[41]

1. Taking into account the nature, size, context and purpose of the processing, as well as the risks and probabilities of the rights and freedoms of natural persons, the healthcare provider shall take appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the processing is carried out in accordance with the GDPR. These dispositions are evaluated and updated when necessary.
2. Where proportionate to the processing activities, the measures referred to above shall include an appropriate data protection policy implemented by the healthcare provider.
3. Coherence with the approved codes of conduct or approved certification mechanisms can be used as an element to show that the obligations of the healthcare provider have been fulfilled.

4.2 Data protection through design and standard settings (Privacy by design and default)[42]

1. Taking into account the state of the art, the implementation costs, and the nature, scope, context and purpose of the processing, as well as the risks and risks inherent in probability and severity for the rights and freedoms of natural persons involved in the processing, the healthcare provider will take appropriate technical and organizational measures, such as pseudonymisation, which have been drawn up with the aim of implementing the data protection principles, such as minimal data processing, in an effective manner, both when determining the processing means and the processing itself, to incorporate the necessary safeguards in the processing as to comply with the requirements of this Regulation and to protect the rights of the data subjects.
2. The healthcare provider shall take appropriate technical and organizational measures to ensure that in principle only personal data that are necessary for each specific purpose of the processing are processed. This obligation applies to the amount of collected personal data, the extent to which they are processed, the period for which they are stored and their accessibility. In particular, these measures ensure that personal data are in principle not made available to an unlimited number of natural persons without human intervention.
3. An approved certification mechanism can be used as an element to demonstrate compliance with the requirements.

Practical implementation:
a) The healthcare provider applies the standards of NEN 7510, 7512 and 7513 for the safe processing of care data.
b) For the provision of data via e-mail, use is made of the secure e-mail connection <evt. name>.
c) The healthcare provider operates according to the 'Personal Data Security Guidelines' of the Dutch Data Protection Authority and the 'Practice Guide patient data in the cloud' of the Dutch Data Protection Authority.
d) The identifying data are stored separately from the content data as much as possible, pseudonymised or encrypted.
e) The default settings are no, unless (opt-in) instead of yes, provided (opt-out), unless the legislation allows opt-out.

[41] Article 24 GDPR
[42] Article 25 GDPR

f) The healthcare provider applies an authorization protocol per processing. It states which data can be processed by whom / which (groups of) employees and why and what powers they have with regard to which data (access, add, modify, delete).

4.3 Joint controllers[43]

1. When two or more controllers jointly determine the purposes and means of the processing, they are joint controllers. They shall determine their respective responsibilities for the fulfillment of the obligations under this Privacy Policy in a transparent manner, in particular with regard to the exercise of the rights of the data subject and their respective obligations to provide the required information, by means of a mutual regulation agreement. A contact point for those involved can be designated in the scheme.
2. It is clear from the regulation in question which role the joint controllers fulfill respectively, and what their respective relationship with the parties involved is.
3. Regardless of such a regulation, a data subject may exercise his rights from the GDPR in relation to and towards each controller.

4.4 Register of processing[44]

1. Healthcare provider must keep a register of the processing activities[45] that take place under their responsibility. That register contains at least the following information:

(a) the name and contact details of the healthcare provider and any joint controller, and of the data protection officer;
(b) the processing purposes;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be provided, including recipients in third countries or international organizations;
(e) where applicable, transfers of personal data to a third country or an international organization, including the indication of that third country or international organization and, in the case of the second subparagraph of Article 49 (1) of the General Administrative Order, intended transfers, the documents on the appropriate safeguards;
(f) if possible, the intended deadlines within which the different categories of data must be deleted;
(g) if possible, a general description of the technical and organizational security measures.

2. The processor and, where applicable, the processor's representative shall keep a register of all categories of processing operations that they have carried out for the benefit of a controller. This register contains the following information:

(a) the name and contact details of processors and of each controller responsible for handling the processor and, where appropriate, the representative of the controller or processor and the data protection officer;
(b) the categories of processing carried out on behalf of each controller;
(c) where applicable, transfers of personal data to a third country or an international organization, stating that third country or international organization

[43] Article 26 GDPR
[44] Article 30 GDPR
[45] Because healthcare providers process special categories of personal data, they are obliged to keep a register of processing operations in accordance with Article 30, fifth paragraph, GDPR. GGZ Nederland has developed a Register Model of Processing Activities with an Explanation Use Model Register of Processing Activities as an example to meet such an obligation. The healthcare provider is free to adjust the model according to his own insight and need within the legal frameworks.

and, in the case of transfers referred to in the second subparagraph of Article 49 (1) of the GDPR, the documents on the appropriate safeguards;
(d) if possible, a general description of the technical and organizational security measures.

3. The register has been drawn up in written form, including in electronic form.
4. If requested, the controller or the processor shall make the register available to the Dutch Data Protection Authority.

4.5 Co-operation / cooperation with the Authority for personal data[46]

The health care provider, the processor and, where applicable, their representatives, shall cooperate, on request, with the Dutch Data Protection Authority in the performance of its tasks.

4.6 Security of processing[47]

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the care provider and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

2. 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, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.
3. Adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements referred to in paragraph 1 of this Article.
4. The healthcare provider and the processor shall take take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is legally required to do so.

4.7 Notification of a personal data breach to the Personal Data Authority (reporting data breaches to the AP) and data breach register[48]

1. 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 Dutch Data Protection Authority, 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 Dutch Data Protection Authority is not made within 72 hours, it shall be accompanied by

[46] Article 31 GDPR.
[47] Article 32 GDPR.
[48] Article 33 GDPR.

reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification to the Dutch Data Protection Authority shall at least describe or communicate the following:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
(c) describe the likely consequences of the personal data breach;
(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The health care provider shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable Dutch Data Protection Authority to verify compliance with this Article.

4.8 Notification of a personal data breach to the data subjects (reporting data leaks to the data subject)[49]

1. When the personal data breach is likely to pose a high risk to the rights and freedoms of natural persons, the healthcare provider shall inform the data subject of the personal data breach without delay.
2. The notification to the data subject shall contain a description, in clear and simple language, of the nature of the infringement in relation to personal data and at least the information contained in the previous article (4.7, third paragraph, under b), c) and d.), the data and measures referred to.
3. The communication to the person concerned shall not be required if any of the following conditions are met:

(a) the healthcare provider has taken appropriate technical and organizational protection measures and these measures have been applied to the personal data covered by the personal data breach, in particular those which render the personal data incomprehensible to unauthorized persons, such as encryption;
(b) the healthcare provider has subsequently taken measures to ensure that the high risk to the rights and freedoms of data subjects is unlikely to materialize;
(c) the communication would require disproportionate efforts. In such a case, a there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the healthcare provider has not yet reported the personal data breach to the data subject, the Data Protection Authority may, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

[49] Article 34 GDPR.

4.9 Data protection impact assessment (Data Protection Impact Assessment, DPIA)[50]

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data[51]. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of[52]:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large-scale of special categories of personal data, such as health data;
(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The assessment shall contain at least:

(a) a systematic description of the intended processing and the purposes of the processing;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

5. When assessing the impact of processing operations carried out by a healthcare provider or processor and in particular for the purposes of a data protection impact assessment, compliance with approved codes of conduct shall be duly taken into account.
6. The healthcare provider will, as appropriate, ask the persons concerned or their representatives, in their opinion, about the intended processing, taking into account the protection of commercial or general interests or the security of processing operations.
7. If necessary, the healthcare provider shall carry out a review to assess whether the processing is carried out in accordance with the data protection impact assessment, at least if there is a change in the risk involved in the processing operations.

4.10 Prior consultation of the Dutch Data Protection Authority[53]

1. The health care provider shall consult the Dutch Data Protection Authority prior to processing where a data protection impact assessment indicates that the processing would

[50] Article 35 GDPR. GGZ Nederland has drawn up a model data protection impact assessment (DPIA) with explanatory notes. See http://www.ggznederland.nl/themas/privacywetgeving or directly via www.ggzdocs.nl
[51] The Dutch Data Protection Authority will draw up a list of the types of processing for which a data protection impact assessment is mandatory. Such a list is not yet available. Article 35, fifth paragraph, GDPR.
[52] Recital (91) GDPR.
[53] Article 36 GDPR. GGZ Nederland has drawn up a job description model job description DPO.

result in a high risk in the absence of measures taken by the controller to mitigate the risk.[54]
2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.
3. When consulting, the healthcare provider shall provide the necessary information as stated in the Privacy Policy. In any case, the following information must be provided:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
(b) the purposes and means of the intended processing;
(c) the measures and safeguards provided to protect the rights and freedoms of data subjects under this regulation;
(d) the contact details of the data protection officer;
(e) the data impact assessment with respect to that processing;
(f) any other information requested by the Dutch Data Protection Authority.

5. Data Protection Officer (DPO)

5.1 Designation of a data processing officer[55]

1. The healthcare provider and the processor shall designate a data protection officer when the healthcare provider or the processor is mainly responsible for a large scale processing of special categories of data, namely for healthcare providers: health data.
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.
3. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks The required expertise and skills include at least:
a) knowledge of national and European privacy laws and regulations on data protection;
b) understanding of the data processing carried out by the organization;
c) understanding of IT and information security;
d) knowledge of the organization and the sector in which it is active;
e) skills to develop a culture of data protection within the organization.
4. The data protection officer may be a staff member of the healthcare provider or the processor or may perform the tasks under a service contract.
5. The healthcare provider or the processor shall publish the contact details of the data protection officer and communicate them to the Dutch Data Protection Authority. for De Regenboog Groep works as a data protection officer: L. Dijkmans fg@deregenboog.org

[54] From recital (94) GDPR it follows that these are situations where the healthcare provider is of the opinion that it is not possible to limit the risk by means of measures that are reasonable in view of the available technology and implementation costs.
[55] Article 37 GDPR. For a model, see job description data protection officer http://www.ggznederland.nl/themas/privacywetgeving or directly via www.ggzdocs.nl

5.2 Position of the data protection officer

1. The healthcare provider and the processor shall ensure that the data protection officer is properly and timely involved in all matters related to the protection of personal data. Specifically, a data protection officer needs, inter alia, the following to fill in the function:
    a) active support from management;
    b) sufficient time to perform the tasks;
    c) sufficient practical support (budget, facilities and staff);
    d) clear communication to all staff about the appointment of the FG;
    e) training.
2. The healthcare provider and the processor shall support the data protection officer in the performance of the tasks referred to below by granting him access to personal data and processing activities and by providing him with the necessary resources for the performance of these tasks and the maintenance of his expertise.
3. The healthcare provider and the processor shall ensure that the data protection officer receives no instructions regarding the performance of those tasks; the data protection officer works independently and independently. The data protection officer shall not be dismissed or punished by the healthcare provider or the processor for the performance of his duties and shall not be adversely affected by the performance of his duties. The data protection officer reports directly to the highest management, board of directors or management, the healthcare provider or the processor.
4. Data subjects may contact the data protection officer on any matter relating to the processing of their personal data and the exercise of their rights under the GDPR.
5. The data protection officer shall be bound to secrecy or confidentiality with regard to the performance of his duties.
6. The data protection officer may perform other duties and duties. The care provider or the processor ensures that these tasks or duties do not lead to a conflict of interest. To prevent conflicts of interest, the data processing officer within the organization may not also have a function in which he determines the purpose and means of data processing. This can be the case, for example, if the data processing officer fulfills a management position, such as head of finance, strategy, marketing, IT or HRM.

5.3 Tasks of the data processing officer

1. The data protection officer shall fulfill at least the following tasks:
    a) the healthcare provider or the processor and the employees who process, inform and advise on their obligations under the privacy legislation (the AVG and other data protection provisions such as from sector-specific legislation and regulations);
    (b) ensuring compliance with this GDPR, other data protection provisions and the policy of the healthcare provider or processor with regard to the protection of personal data, including the allocation of responsibilities, awareness raising and training of the personnel involved in processing and the relevant audits;
    (c) provide advice on the data protection impact assessment and monitor its implementation on request;
    (d) cooperate with the Dutch Data Protection Authority;
    (e) act as a contact point for the Data Protection Authority on processing-related matters, including prior consultation, and, where appropriate, consult on any other matter.
2. The Data Protection Officer shall take due account in the performance of his duties of the

risk involved in processing operations and of the nature, size, context and processing purposes.

5.4 In case of a complaint

In the event of a complaint about the compliance with these regulations, the person concerned can contact the De Regenboog Group Dealer / Care Provider:
Board: H. Wijnands info@deregenboog.org
The data processing officer: L. Dijkmans fg@deregenboog.org
For other complaints, the person concerned consults the complaints procedure.

5.5 Changes and inspection of these regulations

These regulations apply as of 25 May 2018 and can be found on the website of De Regenboog Groep: www.deregenboog.org