PRIVACY NOTICE

THIS IS THE INTERNAL PRIVACY POLICY OF THE CHIROPRACTOR NOORD

The policy covers the processing, holding and/or sharing of (special) personal data in the context of both care provision and the (internal) business operations of The Chiropractor Noord.
The Chiropractor Noord, as a care provider, is the data controller. The Chiropractor Noord determines the purpose and the means for processing (special) personal data. This document describes how The Chiropractor Noord as the data controller handles (special) personal data, so as to comply with the requirements of the General Data Protection Regulation (GDPR).
The following topics are covered in this document:
1 - Updating and compliance check of privacy policy
2 - Categories of personal data and purposes
3 - Organizational and technical measures/security
4 - Duty to inform
5 - Processing register
6 - Information processors and recipients
7 - Retention periods
8 - No Data Protection Impact Assessment (DPIA) for now
9 - Transfer outside the EU
10 - No Data Protection Officer
11 - Security incidents
12 - Rights of all involved
The processing of personal data within The Chiropractor Noord must remain in compliance with the GDPR and with any regulation and legislation that supplements, amends or replaces the GDPR. For this reason, the privacy policy will be evaluated periodically and adjusted as necessary. Likewise, it will be periodically checked whether the privacy policy is complied with by employees and information processors of The Chiropractor Noord.
The Chiropractor Noord processes personal data from the following categories of people:
3.1: (potential) clients
3.2: Parents/caregivers of underage clients
3.3: Visitors of www.thechiropractornoord.nl
3.4: Employees
3.5: Contractors individuals working at The Chiropractor Noord
3.6: Applicants
3.7: All other individuals who contact The Chiropractor Noord or whose personal data The Chiropractor Noord processes.
3.1 Potential clients: The Chiropractor Noord processes personal data of potential clients, for the purpose of identifying the client and executing the healthcare agreement. Identification involves the name, contact and address details, date of birth, and client's citizen service number. This is processed for the execution of the healthcare agreement. Other (special) personal data may also be processed for this purpose; such as medical data.
3.2 Parents/caregivers of underage clients: The Chiropractor Noord processes the personal data of the parents/caregivers of clients, for the purpose of contacting the client and executing the treatment agreement. This involves name and contact details and any financial data such as a bank account number for the billing process.
3.3 Visitors of www.thechiropractornoord.nl: The Chiropractor Noord processes personal data that has been generated during a visit by a data subject to The Chiropractor Noord's website, such as the IP address, the browsing behavior on the website such as data about the first visit, previous visit and current visit, the viewed pages and the way in which the website is navigated and which parts of it the data subject clicks on. These user statistics can be processed into generic reports, which cannot be traced back to individual visitors. This mainly aims to improve the practice website www.thechiropractornoord.nl. Furthermore, personal data isgenerated when a visitor fills in the contact or registration form on the website. This form is secured. The data is used for the purpose for which the contact or web form serves.
3.4 Employees: The Chiropractor Noord processes the personal data of its employees, insofar as this is necessary for the execution of the employment contract and/or a legal obligation, or if the employee has given consent.
Personnel file:
In the personnel file of each employee, the following data is stored:
- The employment contract and related data, for the purpose of determining and paying out salary. For
- the calculation and payment of the salary and other allowances.
- Copies of diplomas, certificates and other registrations.
- Data on the performance of employees for the purpose of individual performance assessment and
- improvement, specifically for (future) appraisal and performance interviews and guidance trajectories.
- Other data, such as data relating to any complaints, warnings, assessments and absenteeism.

• Obtained consent for processing (special) personal data.

Access to the personnel files is secured. Only Gordon Ryan (owner), has access to the personnel file. Upon request, an employee can view his or her personnel file. Data from
personnel files can also be used as management information.
For each employee, a job description for representation purposes has been published on the website, for which the explicit consent of each employee has been requested and obtained. Data required for payment, participation in courses, training, professional associations and external meetings are processed and stored in the company.

Contractors (ZZP'ers):
The Chiropractor Noord processes and stores the personal data of its contractors (ZZP'ers). In the context of the duty of verification in the (wkkgz), an investigation can be conducted into the suitability of the contractors individual (ZZP'er).
Applicants:
The Chiropractor Noord processes personal data of individuals who have applied to The Chiropractor Noord, such as contact details and information stated in the application letter and CV. This data is processed to assess the suitability of the candidate and to contact a candidate. The data is kept for a maximum of 6 months after the application period.
Other individuals:
In the context of the treatments, The Chiropractor Noord may also use data obtained from other care providers or referrers.
The starting point for The Chiropractor Noord is that no more personal data is processed than is necessary to achieve the purpose for which they were collected, both internally and externally when engaging third parties. For both cases, The Chiropractor Noord has taken appropriate technical and organizational measures to protect personal data against loss or unlawful processing.

The Chiropractor Noord has taken the following internal technical and organizational measures:

4.1 The exchange of confidential information with other care providers must exclusively take place via a secure connection. Emailing with other care providers is only allowed for general communication. Exchange of private data via unencrypted methods is not allowed.
4.2 Confidential information must only be stored in the ICT system of the practice that complies with the GDPR laws and regulations. It is also not allowed to store confidential information on external data carriers, unless necessary and the data is encrypted.
4.3 The practice ensures that passwords for the practice's ICT system are sufficiently strong and are changed periodically.
4.4 It is not allowed to leave equipment such as laptops, tablets and mobile phones with special patient data unattended outside the practice. Access to the devices must be protected with passwords.
4.5 Login details must be treated confidentially and must not be shared with third parties. Login details may only be shared confidentially with colleagues in a secure environment without third parties, such as in the case of training a new colleague.
4.6 On leaving the practice, each employee must fully log out of their laptop, shut it down and safely store anypaper files.
4.7 Without the permission of the Practice Manager or practice owner, it is not allowed to download software onto practice devices or to modify or remove firewalls or virus scanners.
4.8 A home computer of the practice must be secured by a password. Security updates must be carried out promptly. No connection may be made via public Wi-Fi networks. It is not allowed to leave information carriers with confidential data unattended in a car or elsewhere outside the practice.
4.9 On leaving the practice, it must be checked whether there are still other people in the building. The last employee present checks whether all windows and doors are closed/locked.
4.10 Access to the building is only possible with keys provided to employees. Keys may not be given to third parties.
4.11 Staff are contractually obliged to maintain confidentiality. The Chiropractor Noord monitors compliance with the above measures. Random (proportional) checks may be carried out. If it is suspected that measures are not being observed by an employee, targeted checks of the employee in question may be carried out. After this check, The Chiropractor Noord may decide on the basis of the findings to take employment law measures.

5. We process only personal data that is strictly necessary for the intended purpose. When developing or purchasing new systems and processes, privacy is considered from the initial design phase (privacy by design). Default settings are configured to ensure that only the minimum required data is processed (privacy by default). We review annually whether the processed data remains necessary and adjust systems and processes where required.
• You may object to the way we process your personal data.
• You may withdraw your given permission that allows us to process your personal data. When you do so, we are (or may) not be able to provide you with the most appropriate care. We will continue to store your data in an inactive archive.

6 - Information processors:
With information processors (Practicehub), The Chiropractor Noord has chosen a company that can encrypt information for processing and storage based on technical and organizational measures. The processor engaged by The Chiropractor Noord is obliged to provide all information to demonstrate compliance with security for the purpose of audits, including inspections. Either by The Chiropractor Noord itself or by an auditor authorized by The Chiropractor Noord.
The Chiropractor Noord informs all involved about how personal data is handled. For this reason, an external privacy statement has been prepared for individuals who are not affiliated with The Chiropractor Noord. This privacy statement is published on The Chiropractor Noord's website.
On joining the company, new employees are informed about the processing of their personal data within The Chiropractor Noord. The internal privacy protocol applies to employees. This internal protocol of The Chiropractor Noord is also included in the practice's ICT system.
The Chiropractor Noord uses external service providers in the processing of personal data. These service providers only process personal data on The Chiropractor Noord's instructions. The Chiropractor Noord has entered into a contract with these parties, which includes a duty of confidentiality.

The Chiropractor Noord uses the following data processors:
- Practicehub (for the purpose of an electronic patient file)
- Google (for email, calendar and Google Drive documents)
- Right eye (for testing)
- Pumble (internal encrypted communication)

7. We store your personal data only for as long as it is necessary for us to provide you with the most appropriate care. We do this according to the legal holding period stated by the ‘Medical Treatment Contracts Act’.
- Medical records: 20 years
- Financial records: 7 years

Deletion is checked annually.

8. The Chiropractor Noord provides personal data to information processors when necessary in the context of executing the treatment agreement or in the case of a legal obligation. Beyond that, no personal data is provided to third parties without the prior explicit consent of the data subject.
In exceptional cases, a DPIA could be carried out by The Chiropractor Noord. The likelihood of necessity is negligible, as contracted data processors are used.

9. In principle, The Chiropractor Noord does not transfer special personal data to countries outside the EEA. When necessary, this is done within the rules of the GDPR and the European Commission.

10. A data controller is required to assign a data protection officer in the case of large-scale data processing. This mainly applies to organizations that are primarily and extensively involved in the processing of special personal data (such as medical data).
'Mainly involved' refers to the core activities of the data controller. The Article 29
Working Party defines core activities as processes that are essential to achieving the objectives of the organization, or that are part of the organization's main tasks. The Chiropractor Noord has not appointed a Data Protection Officer as no large-scale processing of special personal data is involved.

11. The Chiropractor Noord takes security incidents seriously. The organization has taken appropriate technical and organizational measures aimed at minimizing the chance of loss or unlawful processing of personal data as much as possible. Despite these measures, there is a chance that an incident involving personal data may occur. To ensure that action can be taken as quickly as possible to end the incident and limit the damage as much as possible, the following procedure must be followed

In every incident involving personal data, The Chiropractor Noord will assess:
- Whether there is an incident involving special personal data
- What measures need to be taken to end the incident and limit its consequences.
- Whether the involvement of an external party is required to assist in resolving the incident.
- Whether the incident needs to be reported to the AP
- Whether the persons to whom the personal data relates need to be informed about the incident.
- What measures need to be taken to prevent a recurrence of the incident.

The Chiropractor Noord documents breaches involving personal data in the AP's data breach register.

In case a data processor is a potential incident of which the external data processor has become aware earlier, the cooperation agreement stipulates that the processor must inform us of the potential data breach. It is also agreed that both parties will do their best to prevent/resolve
the incident.

12. The rights that a data subject generally has under the GDPR are the right to access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object and the right not to be subject to automated individual decision-making. Through its data processors, The Chiropractor Noord has taken technical measures to enable a justified exercise of these rights. Requests from all involved relating to personal data are handled by the Owner or Practice Manager.

Requests and their handling are saved in the ICT system
Upon receipt of a request, The Chiropractor Noord will do its best to establish the identity of the requester, on the basis of the requester's name, contact and address details.
Once the identity of the requester has been established, The Chiropractor Noord will confirm to the requester that a response will be given to the request within a month. If it turns out that the request is complex, this term can be extended by a maximum of two months. The Chiropractor Noord will inform about the extension of the terms within the first term.
The Chiropractor Noord determines which right the requester invokes and collects the necessary data for this purpose. The Chiropractor Noord assesses whether the requester's request can be met, also considering professional secrecy and legal retention obligations. The practitioner records his findings in a report. The report is stored in the ICT system.
In principle, the applicant will not be charged for processing the request. Nevertheless, the requester may be charged a reasonable fee based on administrative costs, for example in the case of repeated (unfounded) requests or if more than one copy of the file is required.
If the request is granted and the request pertains to rectification, erasure or restriction of processing, the external parties who have received the personal data must also be informed of the request. The Chiropractor Noord determines whether this is the case and notes the third party in the report. Such notifications to external parties are omitted by The Chiropractor Noord if this proves impossible or requires disproportionate effort.