Privacy Policy for Visitors and Users of the Provet.com Website (US Edition)

This privacy policy ("Privacy Policy") describes the kinds of data pertaining to individuals ("personal data") that Nordhealth Finland Oy ("Nordhealth", "we", "our", "us") collects when you visit our website or use our search and booking service at provet.com (collectively, the "Service"); how we use, process, disclose and secure that personal data; and the choices and rights you have regarding your personal data.

Last updated: 16 June 2025

Introduction

Definitions used in this Privacy Policy:

Customer(s): Veterinarians, as well as representatives and contacts of customer organizations such as clinics, who are customers of Nordhealth.

End User: The Customer's own clients, such as pet owners

End User Data: Personal data as defined in the contract between the Customer and Nordhealth, e.g. pet owner's data.

Service Users: An individual visiting or using the Service.

This Privacy Policy only applies to you when you are acting as a "Service User," and does **not** apply to personal data collected from anyone acting as a "Customer" or "End User". We process End User Data on behalf of our Customers as a data processor. If you are an End User and have questions about how our Customers process your data, or if you wish to exercise your rights in relation to such data, you should contact the Customer with whom you booked your appointment. The privacy policy for Customers can be found here: https://my.provet.com/documents/privacy-notice-us.pdf.

For Service Users located in the United States, Nordhealth processes personal data in accordance with applicable U.S. federal and state privacy laws. This Privacy Policy supplements, and does not limit, any non-waivable rights under those laws.

1. Data Controller[1]

Nordhealth Finland Oy is the data controller for the processing described in this Privacy Policy on a global basis. No U.S. subsidiary currently acts as a separate controller or service provider for these activities.

2. Contact Details

Nordhealth Finland Oy (Business ID: 1733917-4)
Bulevardi 21

[1] **U.S. role.** For purposes of applicable U.S. state privacy laws, Nordhealth acts as a "business" (CA) and "controller" (CO/CT/VA/OR/TX) with respect to personal data collected through this website and booking interface.

00180 Helsinki, Finland
Tel. +358 19 425 1610

Email:dpo@nordhealth.com

3. Purpose and Legal Basis for Processing, and Categories of Data Processed[2]

Purpose	Personal Data	Legal Basis
Creating and maintaining a Service User account. From your user account, you can view your previous bookings at different locations and make new appointments with clinics or professionals who use the Service. The Customers act as the data controller for personal data related to the bookings.	Name We do not request Social Security numbers or similar national identifiers for account creation by U.S. Service Users. Contact details (telephone number, email address, postal address)	Contract
Development of our Service	Data collected through cookies and forms, such as IP address, language preference, browser and device type, country of browsing, operating system, search terms, search history, pages visited, frequency of visits, and other information about on-site activities	Legitimate interest in improving Service, including website experience
Prevention and correction of technical problems and errors in our Service, including the website	Data collected through cookies and forms, such as IP address, language preference, browser and device type, browsing country, operating system,	Legitimate interest in ensuring the proper functioning of our Service, including the website

[2] **U.S. categories.** For California and other U.S. state laws, the data elements described in this Section fall within the following categories of personal data: identifiers (e.g., name, contact details), internet or other electronic network activity information (e.g., browsing and usage data), and limited geolocation data (general location derived from IP address). We do not collect sensitive personal data (as defined by applicable law) via this Service, nor do we collect Social Security numbers or similar national identifiers.

	and other information about on-site activities	
Ensuring the security of our Service and preventing misuse	Log data Data collected through cookies, such as IP address, browser and device type, browsing country, and operating system.	Legitimate interest in maintaining the integrity of our Service

Note for U.S. users. We do not collect or request Social Security numbers or similar national identifiers from U.S. Service Users. We also do not collect sensitive personal data (as defined by applicable U.S. state privacy laws) through the Service. If we were in the future to collect sensitive personal data, we would disclose it in this Privacy Policy and you would have the right to limit the use and disclosure of such information.

We do not offer financial incentives related to the collection or use of personal information.

4. Sources of Data

We collect personal data directly from you in connection with your use of the Service.

We may also collect personal data from you if you contact us via email, social media or mail.

We may also collect or verify contact details from publicly available sources and reputable data providers, in compliance with applicable law.

5. Disclosures and International Transfers

We use service providers (sub-processors) for hosting, analytics, communications, support, and security. Core systems are hosted in the EU/EEA, and certain providers may process limited personal data in the United States or other jurisdictions. Where personal data is transferred outside the EU/EEA, Nordhealth implements appropriate safeguards (including the EU Standard Contractual Clauses) and, where relevant, additional transfer protections to ensure an adequate level of protection. A list of key sub-processors is available on request. Where required, we conduct transfer risk assessments and implement supplementary measures to protect personal data transferred to the United States and other third countries.

6. Data Security and Retention

Only employees who, by virtue of their duties, are authorized to process personal data are permitted to access systems containing personal data. The data is technically protected, and access requires appropriate user rights. Firewalls and other technical safeguards are also designed to prevent unauthorized use. Only designated individuals are authorized to process and maintain the personal data, and employees are bound by confidentiality obligations. The information system is securely backed up and can be restored if necessary. Security audits are carried out regularly.

We retain personal data as required by applicable legislation. The necessity of retaining personal data is reviewed on a regular basis in accordance with applicable laws.

In addition, we take reasonable steps to ensure that no incompatible, outdated, or inaccurate personal data is stored in the register, considering the purpose of the processing. Upon becoming aware of incompatible, outdated or inaccurate personal data, we promptly correct or delete such data, as appropriate.

While we apply administrative, technical, and organizational safeguards to secure personal data, no method of transmission or storage is 100% secure. We periodically review and update our data security controls.

We retain website-interaction data for as long as needed to provide and improve the Service and for a reasonable period thereafter for security, legal, and recordkeeping purposes, unless a longer retention period is required or permitted by law. We may retain minimal records (for example, your email address and opt-out status) to comply with legal obligations and to maintain suppression lists, ensuring that we do not send you marketing communications after you opt out.

7. Your Rights as a Data Subject

Certain jurisdictions provide you with particular rights as to your personal data. We permit all of our Service Users to exercise the following rights:

- Right of access to your personal data and to obtain a copy.
- Right to rectification or, in some cases, erasure.
- Right to modify or delete your own profile data.
- Where processing is based on consent, right to withdraw or amend consent (without affecting prior lawful processing).
- Right to data portability and restriction of processing in certain situations.
- Right to object to processing based on legitimate interest, by specifying your particular situation.
- Right to object to processing for direct marketing.

U.S. state privacy rights (where applicable). Depending on your U.S. state of residence and to the extent such laws apply to Nordhealth's processing, you may have additional rights to access, correct, delete, or obtain a copy of certain personal data, and to opt out of certain processing, as described below. You can submit a request using the contact details in Section 2[3].

We will verify your request by matching the information you provide with information we maintain, and may request additional information to confirm your identity.

---

[3] **How to exercise U.S. rights; verification; appeal.** You may submit a request to exercise applicable U.S. privacy rights by emailing dpo@nordhealth.com with "U.S. Privacy Request" in the subject line and your name, email address, and the right(s) you wish to exercise. You may also write to us at the address set forth in Section 2 above. We will take reasonable steps to verify your identity and may request limited additional information for such purpose. Where permitted, you may authorize an agent to submit a request on your behalf if we can verify your identity and receive the agent's written authorization. We will not discriminate against you for exercising any rights provided by law. If we delete your personal data, however, you may not be able to use certain features of the Service. If we deny your request in whole or in part, you may appeal by replying to our decision email with "Appeal" in the subject line. We will review and respond within the timeframe required by law.

We will not discriminate against you for exercising your privacy rights.

Browser signals. We do not recognize browser-based opt-out signals. Because we do not sell or share personal information for cross-context behavioral advertising, we are not required to recognize Global Privacy Control (GPC) signals.

“Sale”/”Sharing”. Nordhealth does not sell personal data and does not engage in cross-context behavioral advertising for this Service. However, if we were to go through a business transition, such as a merger, acquisition by another company, or sale of all or a portion of our assets, your personal data might be among the assets transferred.

Sensitive personal data. We do not collect sensitive personal data.

We do not engage in automated decision-making or profiling with legal or similarly significant effects.

Right to lodge a complaint with the Finnish Data Protection Ombudsman (www.tietosuoja.fi). U.S. residents may also contact us first via Section 2 if they have questions or concerns about our handling of personal data. We will review and respond in accordance with applicable law.

8. No Children.

Our Service is not directed to children under the age of 18, and we do not knowingly collect personal information from children under 18. If you are a parent or guardian and believe that your child under 18 has provided personal information to us, please contact us immediately at dpo@nordhealth.com with "Child Privacy" in the subject line. You may also write to us at the address set forth in Section 2 above. If we learn that we have collected such information, we will delete it.

9. Updates to This Privacy Policy

We regularly review this Privacy Policy and update it from time to time. The Privacy Policy may be updated, for example, if our processing activities change or if applicable data protection laws or guidelines are amended. The updated version of the Privacy Policy will be published on our website and will be effective when published. If we make material changes to this Privacy Policy, we will provide notice before or as soon as the changes take effect (for example, by email or a website banner). This ensures transparency consistent with applicable U.S. and international privacy laws.

10. Contact

All contacts and requests relating to this Privacy Policy should be sent to the contact information in Section 2.

11. Cookies

We disclose identifiers and internet activity information to hosting providers, analytics providers, security vendors, and service providers who assist in operating the Service. Further information on cookies and their use in the Service is available in our Cookie Policy: https://www.provet.com/legal/cookie-policy.

12. State-Specific Privacy Notices

This section supplements our Privacy Policy and provides specific disclosures required by U.S. state privacy laws, including the California Consumer Privacy Act (CCPA) as amended by the CPRA, and comprehensive privacy laws in Colorado, Virginia, Connecticut, Utah, Texas, Oregon, Montana, and others.

A. California Residents (CCPA/CPRA)

1. California residents. If you are a California resident and wish to contact the California Department of Consumer Affairs about this Privacy Policy or our data practices, you may reach them at 1625 North Market Blvd., Suite N-112, Sacramento, CA 95834, or +1 (800) 952-5210.

2. Notice at Collection

In the preceding 12 months, Nordhealth has collected the categories of personal information listed under section 3. We retain this data for as long as necessary to provide our services and comply with legal obligations.

Identifiers and internet/network activity data are retained for as long as necessary to operate the Service and for related security and recordkeeping obligations

2. Your California Rights

California residents have the specific right to:

- **Opt-Out of "Sharing":** You may opt out of the sharing of your personal information for cross-context behavioral advertising.
- **Limit Use of Sensitive Personal Information:** You have the right to limit the use of sensitive personal information to that which is necessary to perform the services. (Note: We primarily process such data only as a processor for our clients).
- **Non-Discrimination:** We will not discriminate against you for exercising your CCPA rights.

California residents have a right to know the personal data we have collected about them, a right to delete that data, and a right to correct inaccurate information.

California Civil Code Section 1798.83 permits California residents to request a list of third parties to whom we have disclosed personal information for their direct marketing purposes during the preceding calendar year. To make such a request, please contact us at dpo@nordhealth.com. You may also write to us at the address set forth in Section 2 above.

B. Colorado, Virginia, Connecticut, Texas, Utah, Oregon, and Montana

Residents of these states have rights similar to those described above.

2. Sensitive Data

We do not collect sensitive data.

3. Appeals

If we decline to take action on your privacy request, we will inform you of the reason within 45 days. You may appeal our decision by replying to our denial email or contacting dpo@nordhealth.com with "Privacy Appeal" in the subject line. You may also write to us at the address set forth in Section 2 above.

- **Timeline:** We will respond to your appeal within 45 days (or 60 days where permitted by your state's law).
- **Escalation:** If your appeal is denied, you may have the right to submit a complaint to your state's Attorney General.

C. Nevada Residents

Nevada law (SB 220) gives Nevada consumers the right to opt out of the sale of certain covered personal information. Although we do not currently sell data as defined broadly by Nevada law (exchange for monetary consideration), you may submit a request to opt out of any potential future sales by emailing dpo@nordhealth.com. You may also write to us at the address set forth in Section 2 above.