	Novellas Healthcare Policy: Data Protection		
	Document No: Version No:	POL-NH-003 2.3	Effective Date Last Review Date:

Data Protection Policy

REVISION HISTORY

This Data Protection Policy is reviewed to ensure continuous relevance to the systems and processes that it describes and a record of contextual additions or omissions is given below:

Ver. No.	Description of Change(s)	Effective Date
1.0	This is a new Policy	22-FEB-21
2.0	Policy updated to reflect that Novellas Healthcare now has a Data Protection Officer (DPO) appointed and some small updates made on the legal basis for the processing of the personal data in section 5.5	30-JUN-21
2.1	References to other Novellas Healthcare procedures/ policies have been made	30-JUN-22
2.2	Review of the POL: <ul style="list-style-type: none"> ➤ adaptation scope ➤ General update 	29-APR-24
2.3	Review of the POL: <ul style="list-style-type: none"> ➤ Administrative update Data Protection principles ➤ Core tasks of DPO added 	23-MAY-2026

1.0 INTRODUCTION AND PURPOSE

Novellas Healthcare will maintain the highest level of respect to protect personal data. We have adopted this Data Protection Policy to support our commitment to protect personal data in accordance with the General Data Protection Regulation of April 27th, 2016 (hereafter the “GDPR”) and national privacy legislation. Novellas Healthcare is ultimately responsible to ensure it meets its legal obligations with regards to Personal Data Protection.

2.0 SCOPE

Our Data Protection Policy applies to all managers, employees, contractors and freelancers (“Staff”) of Novellas Healthcare and its affiliates and is communicated to all Staff throughout the organization via regular communication and/or training. It also applies to all service providers of Novellas Healthcare unless specifically mentioned otherwise.


All Novellas Healthcare Staff have the responsibility to ensure that Personal Data are processed appropriately and must ensure that Personal Data are handled and processed in line with this Policy, related processes to comply with the GDPR data protection principles, and that potential Data Breaches are reported immediately.

3.0 GLOSSARY of TERMS

Anonymized Data	Refers to information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.
------------------------	---

Controller	The natural or legal entity or other body, which alone or jointly with others (“Joint-Controllers”) determines the purposes and means of the processing of Personal Data.
Data Breach	A Data Breach occurs when the data for which Novellas Healthcare is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity.

Data Protection Impact Assessment (DPIA)	A process to help you identify and minimize the data protection risks of a project. You must do a DPIA for data processing that is likely to result in a high risk for individuals.
Data Protection Authority	The National Authority for protection of Personal Data. The Data Protection Authority is an independent body that ensures that the basic principles of personal data protection are properly observed.
Data Protection Officer (DPO)	The primary role of the data protection officer (“DPO”) is to ensure that her organisation processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.
Data Register	A registry in which all purposes for which Personal Data processed by Novellas Healthcare are listed, as well as an overview of which data is collected per data processing.
Data Subject	An identified or identifiable natural person whose information is being processed.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Personal Data	Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which combined together can lead to identification of an individual.
POL	Policy
Processor	A natural or legal entity, public authority, agency or other body, which processes Personal Data on behalf of, and in accordance with the instructions of the Controller.
Pseudonymized Personal Data	The Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural Person.
Special Categories of Personal Data/Sensitive Personal Data	Personal Data that are according to their nature sensitive, more specifically revealing: <ul style="list-style-type: none"> - Race or Ethnicity - Political Preference - Religious or philosophical conditions - Membership of a Union - Genetic Data - Biometric data to identify a person - Health data - Sexual behaviour /preference
Staff	All people working for Novellas Healthcare including Managing Partners, managers, employees, contractors and freelancers.
Service Desk	Service Desk providing ICT support for Novellas Healthcare.

	Novellas Healthcare Policy: Data Protection			
	Document No:	POL-NH-003	Effective Date:	23-MAY-26
	Version No:	2.3	Last Review Date:	22-APR-26

4.0 PROCEDURES

4.1 Definition of Personal Data

Personal Data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

In addition to general Personal Data, there are special categories of Personal Data (also known as Sensitive Personal Data) which are highly relevant because they are subject to a higher level of protection. These data include genetic, biometric and health data, as well as Personal Data revealing racial and ethnic origin, political opinions, religious or ideological convictions or trade union membership.

Personal Data that has been de-identified, encrypted or pseudonymized can be used to re-identify a person remains Personal Data and falls within the scope of the GDPR.

Personal Data that has been rendered anonymous in such a way that the individual is not or no longer identifiable, is no longer considered personal data. For data to be truly anonymized, the anonymization must be irreversible (see also SOP-NH-016: Anonymization and Pseudonymization).

The GDPR protects Personal Data regardless of the technology used for processing that data – it applies to both automated and manual processing. It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, Personal Data is subject to the protection requirements set out in the GDPR.

4.2 Data Protection Principles

Article 5 of the GDPR requires that Personal Data shall be processed in accordance with the following principles:

➤ [Lawfulness, fairness and transparency](#)

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject, At the time of providing personal information, individuals are made fully aware of who is collecting the information, how the information will be used and to whom the information will be disclosed. If Sensitive Data is processed (eg. health related data), explicit consent specifically for that data has to be given.

➤ [Purpose limitation](#)


Personal Data shall collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Personal Data may only be kept for a specific, lawful and clearly stated purpose and may not be used for any other purpose.

➤ [Data minimisation](#)

Personal Data shall be adequate, relevant and limited for the purposes for which they are processed. The collected Personal Data should be enough to achieve its purpose, and no more. It is not allowed to collect Personal Data not needed, "just in case" a use can be found for the data in the future.

➤ [Accuracy](#)

Personal Data collected by Novellas Healthcare should be accurate and up-to-date. If a Data Subject informs Novellas Healthcare of any changes to their Personal Data, Novellas Healthcare should promptly amend those records. The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request for rectification verbally or in writing.

	Novellas Healthcare Policy: Data Protection			
	Document No:	POL-NH-003	Effective Date	23-MAY-26
	Version No:	2.3	Last Review Date:	22-APR-26

You have one calendar month to respond to a request. This request must be forwarded to privacy@novellashealthcare.com and will be logged in the Data Subject Access Request log.

➤ **Storage limitation**

Personal Data shall not be kept longer than necessary for the purposes. If there is no good reason for retaining Personal Data, then that information should be routinely deleted and in accordance with the applicable retention periods. Exceptions may apply, but must always be checked with the DPO.

➤ **Integrity and confidentiality**

Appropriate technical and organisational measures must be taken against unauthorized access to, or unauthorized alteration, disclosure or destruction of the Personal Data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.


➤ **Accountability**

Novellas Healthcare is responsible for and must be able to demonstrate compliance with all of the above principles

4.3 General Guidance

General guidance to ensure Personal Data Protection within Novellas Healthcare:

- Access to Personal Data should be restricted in line with the computerized access restrictions described in “POL-NH-005 ICT Policy”.
- Personal Data stored on paper or removable digital media (eg. CD-rom, DVD or USB-stick), should be kept in a secure place where unauthorized people cannot see/access them, as described in “POL-NH-005 ICT Policy”.
- Personal Data printouts should be shredded and disposed of securely when no longer required.
- Personal Data should never be disclosed to unauthorized people, either within the company or externally. Personal Data sharing via e-mail communication should be avoided as much as possible, or appropriate security measures should be implemented (eg file encryption/password protection).
- When working with Personal Data, Novellas Healthcare Staff should ensure the screens of their computers are locked when left unattended.
- Personal Data should not be shared informally. When access to confidential information is required by certain people, it can be requested and discussed with the relevant Novellas Healthcare Management members (eg General Manager, Quality Manager,...).
- Personal Data should be regularly reviewed and updated if it is found to be out of date.
- In case of suspected Data Breach involving Personal Data, the Data Protection Officer and General Manager (directly or via the line manager) are to be informed immediately upon notification of the suspected breach (see also SOP-NH-012 Data Breach).
- Personal data should never be transferred outside of the EU/European Economic Area (EEA), unless the organization/third party falls under the jurisdiction of an EU GDPR White List country or unless a data processing agreement is in place with the receiver including appropriate technical and organisational measures that ensure GDPR requirements are met.
- Novellas Healthcare Staff should pay special attention when processing Personal Data of special categories or sensitive personal data, except for anonymized data (as these are no longer considered Personal Data under the GDPR). These data can only be processed when explicit consent was obtained from the Data Subject(s).

	Novellas Healthcare Policy: Data Protection		
	Document No: Version No:	POL-NH-003 2.3	Effective Date Last Review Date:

4.4 Organizational and Technical Measures

4.4.1 Data Protection Officer

In order to have a central point of contact for all Staff, Novellas Healthcare has assigned a Data Protection Officer.

The core tasks of the Data Protection Officer are as follows:

- **Information & Advice:** Informing and advising the controller/processor and employees of their obligations under GDPR and other data protection laws.
- **Compliance Monitoring:** Monitoring internal compliance with regulations, policies, and procedures, including auditing and monitoring, training staff involved in processing.
- **DPIA & DPA Guidance:** Providing advice, upon request, regarding Data Protection Impact Assessments (DPIAs) and Data Processing Agreements (DPA) and monitoring their performance.
- **Contact Point (Authority):** Acting as the point of contact and cooperating with the supervisory authority/data protection authority.
- **Data Subject Liaison:** Serving as the point of contact for individuals regarding the processing of their data and the exercise of their rights (e.g., access, deletion)
- **Risk Management:** Identifying data security vulnerabilities and evaluating the likelihood and impact of data breaches.
- **Independence:** The DPO must not receive instructions regarding their tasks and reports directly to the highest level of management.
- **Documentation:** Ensuring proper maintenance of records of processing activities

Novellas Healthcare has assigned a formal Data Protection Officer (DPO) as the core activities of Novellas Healthcare consist of processing regular as well as special categories of Personal Data on large scale.

4.4.2 Password Policy


Novellas Healthcare uses individual (personal) accounts for its Staff. A personal (individual) password is required to access a personal account.

All Novellas Healthcare Staff is responsible for the activity that occurs in a Novellas Healthcare system under a personal login and needs to make sure that personal login information is kept secure. It is not allowed to share personal login information with anyone except the Novellas Healthcare service/helpdesk personnel, who may ask for this information in order to allow them to install software or perform maintenance tasks within the Novellas Healthcare ICT account (see also separate Novellas Healthcare ICT- Policy: "POL-NH-005 ICT Policy")

It is important to note that the unauthorised or accidental disclosure of logins and passwords with third parties constitutes a Data Breach and must to be notified to the Line Manager, Data Protection Officer and Quality & Compliance Manager.

4.4.3 Use of Novellas Healthcare ICT Systems and equipment

As a general rule, Staff and Service Providers shall not file and/or store private messages, private files or any other private documents, in any shape or form, on the Novellas Healthcare and/or Client ICT Systems/Equipment.

	Novellas Healthcare Policy: Data Protection			
	Document No:	POL-NH-003	Effective Date:	23-MAY-26
	Version No:	2.3	Last Review Date:	22-APR-26

Work-related e-mail should be accessed via Novellas Healthcare equipment and or Client equipment only. As a general rule, it is not allowed to use personal devices to access or store professional or business-related information. For certain freelancers, there might be an exception to allow use of their own personal device. They must at any time comply with the provisions of this Policy and the Novellas Healthcare security measures by ensuring that professional and business-related information, and more specifically sensitive Personal Data is removed from their device as soon as possible and/or when no longer needed to execute their services for Novellas Healthcare.

4.4.4 Data Security

Physical Security: The owner of personal data/confidential information held in a filing cabinet is responsible for keeping the cabinet locked when not in use. Keys to cabinets holding confidential information should be locked away or kept on person when not in use. If cabinets are locked by numeric code, the code should be kept confidential.

Digital security for sensitive data from Patient Support Programs: Files containing personal data from patients will be stored on a separate folder on the Novellas Healthcare cloud. Access to this folder will be provided by the administrator from the Service Desk of Novellas Healthcare at the request of the Project Manager Patient Support Programs or of the Quality & Compliance Manager. Access will be given at project specific level when Staff starts working on a project. Access will be revoked when Staff does no longer work on a project. Access rights are logged and monitored centrally (see also separate Novellas Healthcare SOP-IT-003 Access Management).

4.4.5 Data Privacy Policy

Novellas Healthcare has a “Privacy Policy” which is publicly available on the Novellas Healthcare website. This policy describes which types of Personal Data are processed by Novellas Healthcare, the purpose of processing Personal Data, as well the Data Subject’s rights and how they can exercise those rights them.

4.4.6 Data Register

To ensure transparency and tracking of processing activities, Novellas Healthcare keeps a Data Register that lists all purposes for which Novellas Healthcare processes Personal Data as well as the information collected for each of those purposes.


4.4.7 Data Breach Register

A Data Breach is a confirmed incident in which Personal Data as well as sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion.

A Data Breach must be reported without delay and within 72 hours of becoming aware of the breach, where feasible (even if not all the details are available yet) to the Data Protection Authority (*in Dutch: 'Gegevensbeschermingsautoriteit', in French: 'L'Autorité de protection des données'*) if there is a risk to the rights and freedoms of individuals..

To ensure transparency, and to keep track of potential Data Breaches, Novellas Healthcare will document any potential Data Breach it becomes aware of in a Data Breach Register. Each potential Data Breach will be investigated, including a risk assessment and will be notified to the Supervising Authority and Data Subject(s) if applicable (*see also separate Novellas Healthcare SOP on Data Breaches (SOP-NH-012)*).

It is the responsibility of each Novellas Healthcare Staff member to identify potential breaches and to report these immediately upon discovery and at the latest within 24 hours after discovery by e-mail to the DPO, the Quality & Compliance Manager and Line Manager.

	Novellas Healthcare Policy: Data Protection		
	Document No: Version No:	POL-NH-003 2.3	Effective Date Last Review Date:

4.5 Which information is collected by Novellas Healthcare and how do we use it ?

Novellas Healthcare collects and uses personal data from Staff, job applicants, partners, patients, business contacts, suppliers, or anyone else who wants to utilize the company’s services and products as well as from anyone who contacts us. Novellas Healthcare may also collect and use personal data from potential customers and/or suppliers. The purpose of processing this Personal Data can vary. However, the Personal Data is always processed with a legal basis, as defined in and in accordance with the provisions in the GDPR.

4.5.1 Employees and Service Providers

Novellas Healthcare has prepared a confidentiality/data protection statement specifically for the company’s Staff as well as for service providers, which is part of the contract between Novellas Healthcare and Staff/service provider. The legal base for this processing can be found in Article 6.1 b) of GDPR: performance of a contract.

4.5.2 Job applicants

For job applicants, we save the Personal Data provided in their application/notice of interest and CV. Novellas Healthcare uses this Personal Data for recruiting purposes. The legal basis for the processing of this personal data is stated in Article 6.1 f) of GDPR: consent. Processing is permitted because the Data Subject has given Novellas Healthcare the permission to use their personal data to handle the application /notice of interest concerning possible employment for Novellas Healthcare or our clients. The applicant is informed about our privacy policy which is also available on our website.

4.5.3 Partners/Business Contacts/Suppliers


For partners/business contacts Novellas Healthcare collects and uses personal data such as company information as well as names and contact information of employees at the company. The data is used to fulfil our contractual obligations with our partners/business contacts. The legal base for this processing activity can be found in Article 6.1 b) of GDPR: performance of a contract.

4.5.4 Patients in our Patient Support Programs

For patients participating in a Patient Support Program, managed by Novellas Healthcare, the treating clinic/doctor collects and uses the patient’s Personal (and Sensitive) Data and clinical information according to applicable laws and regulations. The Novellas Healthcare nurses/care coaches will collect, store, process, and report these data for the purposes as defined in the Patient Support Program. The patient will provide consent by signing an informed consent form explaining the legal background of the collection and processing of Personal Data. The legal basis for the processing of this Personal Data is stated in article 6.1 a) together with article 9.2 a) of GDPR: informed consent. Processing is permitted as a result of the patient’s signed informed consent form.

4.5.5 Potential Partners/Business Contacts/Candidates

Novellas Healthcare collects and uses Personal Data related to potential customers, candidates and, where applicable, suppliers, including company information as well as names and contact information of employees at the company. The data is used for marketing purposes in customer relationship management and to be able to contact prospects.

	Novellas Healthcare Policy: Data Protection			
	Document No:	POL-NH-003	Effective Date	23-MAY-26
	Version No:	2.3	Last Review Date:	22-APR-26

These Personal Data processing activities have their legal basis in Article 6.1 f) of GDPR: legitimate interest. Processing is permitted because it is necessary for meeting our legitimate interest in performing customer relationship management and for contacts with prospects.

4.5.6 Answers to questions

When external people communicate with Novellas Healthcare, we process their Personal Data in the form of name, e-mail address and, in certain cases, telephone number and address of the contacting person as well as any comments this person submits in their communication with Novellas Healthcare. These personal data processing activities have their legal basis in Article 6.1 f) of GDPR: legitimate interest. Processing is permitted because it is necessary for meeting our legitimate interests in handling external people’s questions and comments.

4.5.7 Fulfilling legal obligations

Novellas Healthcare also processes relevant Personal Data to fulfil legal obligations, such as those resulting from payroll, accounting and tax legislation. These Personal Data processing activities have their legal base in Article 6.1 c) of GDPR. Processing is permitted because it is necessary for Novellas Healthcare to fulfil its legal obligations according to the law.

4.5.8 Establishment, exercise and defence of legal claims

Novellas Healthcare may process relevant Personal Data to establish, exercise and defend legal claims in the case of a dispute with an external party/person and Novellas Healthcare. These Personal Data processing activities have their legal basis in Article 6.1 f) of GDPR: legitimate interest. Processing is permitted because it is necessary for Novellas Healthcare to be able to fulfil its legitimate interest in establishing, exercising and defending legal claims.

4.6 How long do we save Personal Data ?

The Personal Data is saved as long as it is needed to fulfil the purposes stated in this Data Protection Policy, unless it is necessary to save the Personal Data for longer than stated in this Data Protection Policy or it is required by law. The following criteria are used to determine how long we save data:


- as long as Novellas Healthcare has an ongoing relationship with the person
- as long as required according to the legal obligations that Novellas Healthcare is bound by (for example account and tax law)
- as long as appropriate in light of Novellas Healthcare’s legal situation

When the Personal Data are no longer required at Novellas Healthcare or have passed the retention period, we will ensure the Personal Data are securely deleted.

4.7 Disclosure and transfer of personal data

Novellas Healthcare may release Personal Data to processors acting on Novellas Healthcare’s behalf as well as to other external parties, such as IT providers or other service providers who process Personal Data according to Novellas Healthcare’s instructions. Data Protection Terms or an equivalent binding document will be signed with that third party as part of or in addition to the respective service agreement.

If the release of Personal Data means transferring it outside the EU/European Economic Area (EEA), Novellas Healthcare will ensure that Standard Contractual Clauses, as created and approved by the Supervisory Authority, are

	Novellas Healthcare Policy: Data Protection			
	Document No:	POL-NH-003	Effective Date:	23-MAY-26
	Version No:	2.3	Last Review Date:	22-APR-26

signed between Novellas Healthcare, as the party sending the personal data, and the external party in question, and/or that other security measures are taken before such a transfer takes place. Novellas Healthcare must always inform the Data Subjects of the transfer of their Personal Data.

Data Subjects have the right, upon request, to obtain a copy of documentation that can prove that appropriate security measures were taken to protect their Personal Data when it was transferred outside the EU/EEA.

Novellas Healthcare might consider it necessary to audit/have an audit performed at a Processor/Sub-Processor of Novellas Healthcare, to check if the respective party has implemented appropriate and sufficient measures to ensure compliance with the GDPR, the applicable national legislation and/or the agreed terms in the Data Processing terms or similar binding document.

4.8 Data Subject Rights

The GDPR provides the following rights for the Data Subject:

- The right to be informed (*e.g. on how the data is processed*)
- The right of access (*e.g. have a copy of the collected data*)
- The right to rectification (*e.g. have the data corrected if it is incorrect or misleading, or to complete the data*)
- The right to erasure (*e.g. the right to “be forgotten”*)
- The right to restrict processing (*e.g. the request us to stop processing*)
- The right to data portability (*e.g. request a machine-readable copy of personal data*)
- The right to object (*e.g. revoke consent; to request that we change the way we/no longer contact the Data Subject for business development or public relations purposes*)
- The right to file a complaint with a Data Protection Authority

The different Data Subject rights are explained in more detail in WI-NH-003 - Handling of Data Subject Access Requests.

To exercise the above rights, the Data Subject can contact Novellas Healthcare at privacy@novellashealthcare.com. The DPO will review all requests and will respond, as foreseen in the GDPR, within one (1) month of the request and will attempt to resolve any complaint related to the use of Personal Data.

4.9 Data Protection Impact Assessment (DPIA)

A DPIA must be carried out when a planned or existing processing operation is likely to result in a high risk to the Personal Data, and hence in a high risk to the individuals. DPIA’s are particularly relevant when introducing a new data processing system or technology.

The DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

The Data Protection Officer will provide advice to the applicable process owner to perform the DPIA as needed.

Appendix A: DPO – Novellas Healthcare Statement

To date, Novellas Healthcare has assigned a Data Protection Officer (DPO) in view of the European General Data Protection Regulation (GDPR), (EU) 2016/679.

This decision was taken based on an evaluation of the criteria below for assessing the requirement of a DPO, as set forward by the Regulation:

Text from Article 29 « Data Protection Working Party », Annex 5 (WP243, rev 01). <i>The designation of a DPO is an obligation IF</i>	Novellas Healthcare Assessment
<i>1) the processing is carried out by a public authority or body (irrespective of what data is being processed)</i>	We are not a public authority or body, so condition is not applicable
<i>2) the core activities of the controller or the processor consist of processing operations which, require regular and systematic monitoring of data subjects on a large scale</i>	Novellas Healthcare is processing Personal Data on a large scale as Recruitment and Patient Support Programs are two of the core businesses.
<i>3) if the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences</i>	As the Patient Support Programs are becoming a bigger and bigger part of the Novellas Healthcare core business, the processing of special categories of personal data is becoming more and more prominent.



Novellas Healthcare Policy: Data Protection

Document No:	POL-NH-003	Effective Date:	23-MAY-26
Version No:	2.3	Last Review Date:	22-APR-26

SIGNATURE PAGE

The signatures below certify that this Data Protection policy has been authorized and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensuring their provision

Date	Written, Reviewed and Signed by
2026-04-22	<i>Inge Wyns</i> _____ Wed, Apr 22, 2026 1:04 PM CEST
	Inge Wyns, Quality and Compliance Manager

Date	Written, Reviewed and Signed by
2026-04-22	<i>Kelly Alix</i> _____ Fri, 24 Apr 2026 13:48 CEST
	Kelly Alix, Data Protection Officer

This document is property of Novellas Healthcare. It must not be reproduced in whole or in part or otherwise disclosed without prior written consent. The official controlled copy of this document is the signed PDF version held within our network server and visible to all authorized users. All printed copies, and all electronic copies and versions, except the ones described above, are considered uncontrolled copies which should be used for reference only