MOVESHELF®

Data Processing Addendum – Moveshelf Labs B.V.

Version: 2021c, Dec 1st 2021

General description

This Data Processing Addendum, together with the Standard Clauses for Processing (Section 2 in our terms, also reproduced as Appendix 2 in this document), constitutes the processing agreement (also called DPA, Data Processing Agreement) for the Moveshelf service. The Standard Clauses for Processing have been drawn up by the industry association NLdigital.

The subjects, goals, category, subprocessors, type of data involved in the processing and the duration of the processing are detailed in Appendix 1.

Signing and submitting

We make it easy for Moveshelf customers to sign and submit our DPA by pre-signing this document. You can sign this document on page 2, and email the signed copy to infosec@moveshelf.com.

Questions

If you have any questions about this DPA or data protection, please contact the Moveshelf infosec team at infosec@moveshelf.com.

Overview of security measures

The following is an overview of the most important security measures adopted by Moveshelf. If you are an information security professional and wish to understand the details of our information security management, please request our Statement of Applicability by emailing to infosec@moveshelf.com. Moveshelf applies at least the following security measures:

- Moveshelf adopts permanent Information Security practices in line with prescription from ISO27001 / NEN7510. Moveshelf regularly works with external Information Security Experts with proven track records that advise and perform yearly security audits to ensure effectiveness of its Information Security practices.
- Moveshelf only relies on subprocessor services which have ISO27001 / NEN7510 certifications (see also Appendix I for details). In compliance with GDPR 28.3, we record contracts that specifically include security and data-protection measures with any relevant third party. Upon first request, these contracts can be offered for review.

- Moveshelf does not rely on local servers to systematically process information from the Controller.
- Moveshelf ensures that processed data is always kept under state-of-the-art encryption, both at rest (AES-256) as well as in transit (HTTPS).
- Certified cloud services and storage services always have physical access protections and clear, safe, and secure media sanitization policies.
- Moveshelf adopts complete data segregation between data from different customers. Data is kept in separate "storage buckets" that meet state-of-the-art security measures.
- Employees only receive rights and logical access to information with a need-to-know and least-privilege principle.
- Moveshelf employees are screened prior to employment by requesting a Certificate of Conduct.
- All Moveshelf employees receive regular information security training, as appropriate for their job description.
- All contracts with Moveshelf employees and contractors contain a confidentiality clause.
- Moveshelf employees do not directly access systems of the Controller.
- Moveshelf adopts standard and state of art logging measures that are in line with requirements from NEN7513. More specifically, Moveshelf relies on https://cloud.google.com/logging/docs/view/logs-viewer-preview and on https://cloud.google.com/error-reporting which, on demand, will provide us required information.
- Moveshelf regularly backups data.
- Moveshelf implements two-factor authentication and single-sign on.
- Moveshelf has a clearly defined incident response and data breach procedure.

Processing within and outside of the EU/EEA:

Data uploaded by customers is processed and stored in the EU/EEA.

Agreed and signed:

Controller:	Processor: Moveshelf Labs B.V.
Name:	Name: Ignazio Aleo, CEO
Place, date:	Place, date: Utrecht, October 22, 2021

Appendix 1 – Types of personal data, purposes of the processing, subprocessors and retention periods

Effective date	Brief description of services	Nature of the act of processing	Type of Personal Data	Categories of Parties Involved	Purposes of the processing	Authorised sub-processors	Agreements regarding retention periods
At the start of the agreed service period.	Moveshelf online data processing and visualization service	Measurement processing and clinical history/schedule analysis	Movement data, electronic health record ID and/or other unique identifiers, relevant medical history, clinical schedule.	Patients	Data processing and aggregated visualization to provide and organize care and research for the Organization	Google, Microsoft	Until 3 months after the end of the agreed service period
At the start of the agreed service period.	Moveshelf online data processing and visualization service	Identification data processing and support	Name, avatar, email address, and/or other unique identifiers.	Employees	Data processing and aggregated visualization to provide and organize care and research for the Organization	Google, Microsoft	Until 3 months after the end of the agreed service period
At the start of the agreed service period.	Moveshelf online data processing and visualization service	Usage metrics	Pseudo-anonymized unique identifier	Patients, Employees	Continuous support and improvements.	Google, Mixpanel.	Until 3 months after the end of the agreed service period

Appendix 2 - Standard clauses on data processing

Article 23 General

23.1 Supplier processes the personal data on client's behalf and in accordance with the written instructions agreed on by supplier and client.

23.2 Client, or client's client, is the controller in the sense of the GDPR, has control over the processing of personal data and has established the purpose of and the means for the personal data processing.

23.3 Supplier is processor in the sense of the GDPR and, for that reason, has no control over the purpose of and the means for the personal data processing and, therefore, does not take any decisions on, amongst other things, the use of the personal data.

23.4 Supplier implements the GDPR as laid down in this section 'Standard clauses on data processing' and in the agreement. Client is responsible for assessing, on the basis of this information, whether supplier offers adequate guarantees with respect to applying appropriate technical and organisational measures for the processing to meet the requirements posed by the GDPR and to adequately safeguard the protection of the data subjects' rights.

23.5 Client guarantees vis-à-vis supplier that it acts in compliance with the GDPR, that its systems and infrastructure are at any time appropriately secured and that the content, the use and/or the processing of the personal data are not unlawful and do not breach any third party rights.

23.6 Client is not entitled to seek recovery from supplier of an administrative fine imposed on client by the supervisory authority, on whatever legal ground. In the present section (Section 2) 'supervisory authority' is understood to mean the supervisory authority referred to in the GDPR.

Article 24 Security

24.1 Supplier takes all the technical and organisational security measures described in the agreement. When implementing these technical and organisational measures, supplier has taken into account the state of the art, the costs involved in implementing the security measures, the nature, scope and context of the processing, the nature of its products and services, the processing risks and the varying risks, in terms of likelihood and severity, posed to the rights and freedoms of the data subjects that supplier could expect in view of the use intended to be made of its products and services.

24.2 Unless explicitly stated otherwise in the agreement, supplier's product or service is not intended for processing special categories of personal data or data relating to convictions under criminal law or criminal offences.

24.3 Supplier endeavours to ensure that the security measures to be taken by supplier are appropriate for the use of the product or service intended by supplier.

24.4 The security measures described offer a security level, in client's opinion and taking the factors referred to in article 24.1 into account, appropriate to the risk involved in processing personal data used or provided by client.

24.5 Supplier may adjust the security measures implemented if this should be required, in supplier's opinion, to continue to offer an appropriate security level. Supplier keeps a record of important adjustments and informs client of these adjustments where relevant.

24.6 Client may request supplier to implement further security measures. Supplier is not obliged to implement any adjustments in its security measures following such request. Supplier may charge client for the costs involved in implementing the adjustments requested by client. Supplier is not obliged to actually implement these adjusted security measures before the security measures requested by client have been agreed on in writing.

Article 25 Personal data breaches

25.1 Supplier does not guarantee that the security measures are effective in all circumstances. If supplier discovers a personal data breach, supplier informs client of this without undue delay. The agreement stipulates in which way supplier informs client of personal data breaches. If no specific arrangements have been agreed on, supplier contacts the client's contact person in the usual way.
25.2 It is up to the controller – i.e. client or client's client – to assess whether the personal data breach reported by supplier must be reported to the supervisory authority or the data subject. Reporting personal data breaches is, at any time, controller's – i.e. client's or client's client's – responsibility. Supplier is not obliged to report personal data breaches to the supervisory authority and/or the data subject.

25.3 Where required, supplier provides further information on the personal data breach and renders assistance in providing the information to client that client needs to report a breach to the supervisory authority or the data subject.

25.4 Supplier may charge client for the costs involved in this context, within reason and at supplier’s current rates.

Article 26 Confidentiality

26.1 Supplier ensures that the obligation to observe confidentiality is imposed on any person processing personal data under supplier’s responsibility.

26.2 Supplier is entitled to provide personal data to third parties if and insofar as this should be required pursuant to a judicial decision or a statutory requirement, on the basis of an authorised order by a public authority or in the context of the proper performance of the agreement.

Article 27 Obligations following termination

27.1 In the event the processing agreement ends, supplier deletes, within the period of time agreed on in the agreement, all personal data received from client that it has in its possession in such a way that they can no longer be used and are rendered inaccessible, or, if agreed on, returns these data to client in a machine readable format.

27.2 Supplier may charge client for any costs possibly incurred in the context of the stipulation in the previous paragraph. Further arrangements on this may be laid down in the agreement.

27.3 The provisions of article 27.1 do not apply if statutory provisions should prohibit supplier to delete the personal data or return these, in part or in full. In such event supplier only continues to process the personal data insofar as required under its statutory obligations. The provisions of article 27.1 do not apply either if supplier is a controller in the sense of the GDPR with respect to the personal data.

Article 28 Data subjects’ rights, Data Protection Impact Assessment (DPIA) and audit rights

28.1 Where possible, supplier renders assistance in reasonable requests by client that are related to data subjects exercising their rights against client. If supplier is directly contacted by a data subject, supplier refers this data subject, whenever possible, to client.

28.2 If client should be obliged under the GDPR to carry out a Data Protection Impact Assessment (DPIA) or a prior consultation following this, supplier renders assistance, at client’s reasonable request, in this DPIA or prior consultation.

28.3 At client’s request, supplier provides all information that would be reasonably required to demonstrate compliance with the arrangements laid down in the agreement with respect to personal data processing, for example by means of a valid Data Pro Certificate or another certificate at least equal to it, an audit report (Third Party Memorandum) drafted by an independent expert commissioned by supplier or by means of other information to be provided by supplier. If client should nevertheless have reasons to assume that the personal data are not processed in accordance with the agreement, client may commission an audit, no more than once per year and at client's expense, by an independent, certified external expert who has demonstrable experience in the type of data processing that is carried out under the agreement. Supplier is entitled to refuse an expert if this expert affects, in supplier's opinion, supplier's competitive position. The audit is limited to verifying compliance with the arrangements on personal data processing as laid down in the agreement. The expert is obliged to observe confidentiality with respect to his findings and only reports issues to client which result in a failure by supplier to meet its obligations under the agreement. The expert provides supplier with a copy of his report. Supplier may refuse an expert, an audit or an instruction by the expert if this should be, in supplier's opinion, in violation of the GDPR or other laws and regulations or if this should be an unacceptable breach of the security measures implemented by supplier.

28.4 Parties hold consultations on the findings of the report as soon as possible. Parties comply with the improvement measures proposed and laid down in the report insofar as this can be reasonably expected from them. Supplier implements the proposed measures insofar as these are appropriate in supplier's opinion, taking into account the processing risks associated with supplier's product or service, the state of the art, the implementation costs, the market in which supplier operates and the intended use of the product or service.

28.5 Supplier is entitled to charge client for the costs it has incurred in the context of the provisions laid down in this article.

Article 29 Subprocessors

29.1 Supplier has stated in the agreement if and, if so, which third parties (subprocessors) supplier contracts for the processing of personal data.

29.2 Client grants supplier permission to contract other subprocessors in the performance of supplier's obligations under the agreement.

29.3 Supplier informs client about possible changes with respect to the third parties it contracts. Client is entitled to object to said change by supplier.