PRIVACY REGULATIONS regarding the Web Health History ("W.H.H.") Service called Lifepassport provided by Meshpass SA

Updated: 20 Jun 2018 (substitutes previous versions)

This Privacy Policy describes the rules and procedures for the collection, use and disclosure of user/party concerned information.

The Lifepassport Service made available by Meshpass SA consists of a private health platform that allows users/parties concerned to collect, edit, integrate, store and share health information online.

Thanks to the Service, the user/party concerned is able to control his/her own health data.

Users/parties concerned may access the service through the Lifepassport website www.lifepassport.org and through applications on devices, API or third-party devices. A "device" is any computer used to access the Lifepassport Service, including, for example, desktops equipment, laptops, mobile phones, tablets and other electronic devices.

"Data processing" means any operation relating to the same, regardless of the means and procedures used, namely the collection, storage, use, modification, communication, archiving or destruction of data.

This Privacy Policy governs the client's access to the Lifepassport Service, regardless of the media through which it is accessed. By using Meshpass services, the user/party concerned consents to the collection, transfer, processing, storage, disclosure and other uses of data described in this Privacy Policy.

All the different data formats, content and information described below are referred to collectively as "information".

Regarding the use of Meshpass services by users, we hereby clarify the way Meshpass uses information and explain how users can protect their privacy.

Meshpass defends the user's privacy with all its skills and undertakes to protect your information from unauthorised access.

All personal data processing activities shall be performed in accordance with applicable legislation on data protection for the purposes for which the information was sent, in particular under the laws of Switzerland. Please read the following carefully to understand our views and practices with respect to the personal data of users and how this data will be processed by us. By ticking the box provided for this purpose, the user accepts the terms of this Policy and consents to the processing and use of his/her personal information as described herein. For the purposes of Swiss legislation on the protection of personal data, the data controller is Meshpass SA.

The data processing complies with the principle of good faith and proportionality, thus the Lifepassport service is provided in accordance with the "principle of **accountability**" by which Meshpass has previously acquired the following security documentation and keeps it up to date:

- security report on the HA Cloud server prepared by the data centre that stores the data;
- "penetration test" certification prepared by the software house that has 27001 certification;

- technical report on the Lifepassport application's data encryption systems and evaluation of automatic programs for the allocation and management of authentication codes;
- summary of firewall intrusion alarms installed by the data centre and on the server machines.

The organisational model of Meshpass provides minimal staff involvement and all the systems engineering is mainly managed through the application's automatic systems.

1. The information we collect and store

Meshpass protects data stored on Lifepassport using the most advanced encryption standard, the same technique used by banks to protect their customer data.

Meshpass uses data encryption except for e-mail messages sent to the user/party concerned.

Meshpass stores data in different data centres located in Switzerland with the most advanced standards of information security and perimeter protection barriers similar to military and video-surveillance systems. It also has professional staff to ensure the protection of its data centres from a physical point of view.

Meshpass also adopts protection systems against Distributed Denial of Service (DDoS), Man in the Middle (MITM) and packet sniffing attacks.

Meshpass keeps redundant backup of all the data in various locations to prevent the remote possibility of data loss.

Information provided by the user/party concerned

When the user/party activates Lifepassport, Meshpass collects the personal information strictly necessary to provide the Service correctly.

The following is the only data visible by Meshpass for the management of individual administrative statuses and for the correct operation of the Service:

1. Full name;
2. Address;
3. Post code;
4. Town;
5. Country;
6. Gender;
7. Date of birth;
8. Language;
9. E-Mail;
10. Mobile Phone Number.
11. Payment data – bank account details, credit card details, etc.

Each user/party concerned is identified by Meshpass via an "Activation Code" which will report all medical and personal information that the user wishes to enter personally and under the responsibility of the user/party concerned.

Any other data entered by the user/party concerned of the Service cannot be read by Meshpass since the computer system is fully encrypted via the breakdown of the data.

Lifepassport may only be accessed using the following univocal codes:

- Private Card;
- Medical Card.

The Lifepassport service can be anonymous since the name and the surname of the owner are not necessarily included in Lifepassport's personal details section.

The email address the user enters when creating his/her account shall only be used by Lifepassport Meshpass to communicate with the user/party concerned.

Files and Records

Meshpass employees cannot view the content of the file that the user/party concerned stores on his/her Lifepassport account. They can only view the metadata of the file (e.g. file names and status). As with most online services, a small number of our employees and collaborators must be able to access the user data for the reasons stated in our privacy policy (e.g. when required to do so by law). However, this is a rare exception, not the rule. We have strict rules and technical controls on access that prevent access to employees and collaborators with the exception of these rare and circumstantial situations. In addition, we employ various measures of physical and electronic security to protect user information from unauthorised access.

Meshpass encrypts files after they have been uploaded and the encryption keys are managed by Meshpass or persons appointed by the same.

At the first access the Service asks the user/party concerned to register in the system by linking his/her master data to the activation code, which is inside the purchased package. The activation code and related Private Card and Medical Card codes are keys to access the Web service, and as such must be carefully looked after.

The user/party concerned may need to provide additional information depending on the system features he/she uses.

Log data
When the user uses the Service, Meshpass automatically records information that may include the IP address (Internet Protocol) address of the device, type of browser, international settings preferences, the identification numbers associated with the devices, the mobile phone operator, the time and date associated with the transaction, information on the system configuration, the metadata associated with the files and other interactions with the Service.

Cookies
Meshpass also uses cookies in order to collect information and improve its Services. A cookie is a small text file stored on the hard disk by a Web page. Cookies cannot be used to run programs or deliver viruses to a computer. A Web server assigns cookies only to the user/party concerned and only the Web server of the domain from which they are issued can read them. One of the main

purposes of cookies is to allow the user/party concerned to save time. For example, if a user personalises a web page, or navigates on a site, cookies store this information for subsequent visits. When the user/party concerned returns to the same website, the information previously provided can be retrieved and customised features are immediately available.

The user/party concerned can configure his/her browser by editing its options so that cookies are not accepted or ask for confirmation before accepting a cookie from the websites visited. However, if the user does not accept cookies, it may not be possible to use of some of the features of the Service. The user/party concerned can also set his/her browser to block all cookies, including those associated with Meshpass services, or indicate when a cookie is set by Meshpass. However, it is important to bear in mind that many Meshpass services may not work properly if cookies are disabled. For example, it may not be possible to store language preferences.

Meshpass does not use or install spyware on the computer of the user/party concerned, or ever use spyware to retrieve information from the computer of the user/party concerned.

Occasionally you may receive cookies from companies that advertise on our behalf or on behalf of our subsidiaries. We do not control these cookies, which are not subject to our Cookies Policy.

Additional information and explanations are provided in the dedicated "Cookies Usage" document.

2. How we use personal data

Personal Data
Meshpass may collect personal information that can be used to contact or identify the user/party concerned while he/she uses the Service ("Personal Information"). Personal information may be used to:

- provide and improve the Service;
- by the user/party concerned, to administer the Service;
- better understand needs and interests;
- customise and improve the experience of the user/party concerned;
- provide or offer software updates or product information;
- determine the age and location of the user/party concerned and check if he/she is entitled to an account or service features, such as a language version.
- Communicate new health or advertising services.

If the user/party concerned no longer wishes to receive communications from Meshpass, the instructions provided in the subscription or update information for account setup communications can be followed.

Meshpass uses the data collected from all of its services to provide, maintain, protect and improve its services, develop new ones and to protect Lifepassport and its users.

Meshapass may process ananymous information also for statistical or research purposes.

Geo-location Information

Some devices allow applications to access information in real time on the basis of a location (e.g. a GPS). Our mobile apps do not collect this type of information on the entry into force of these rules, but may do so in the future, with the permission of the user/party concerned, to improve our services.

Analytical data

Meshpass may also collect certain information (directly or through third-party services) using logs and cookies and correlating them, at times, with the personal information of users. Meshpass uses this information for the purposes set out above, as well as for monitoring and analysing the use of the Service, for its technical administration, to improve the functionality and ease of use of the Service and to check that users have the authorisations necessary for the Service to process their requests. Meshpass does not provide companies, organisations or third parties with personal information, except for situations where the user/party concerned has expressed his/her consent or has expressely delegated decisions.

3. Data Sharing and Disclosure

Use by the user/party concerned
Personal Information shall be displayed in the profile page of the user/party concerned and elsewhere in the Service in accordance with the account settings. All information provided must reflect the degree essential to use the Service. The user should carefully consider what information he/she wishes to disclose and the requried level of anonymity.

The user/party concerned is compeltely responsible for maintenance of the confidentiality of his/her account, including the password, and for any other occurence related to his/her account due to his/her inability to keep data secure and confidential. The user/party concerned undertakes to immediately notify Meshpass of any unauthorised use of his/her account or any other breach of security.

Meshpass shall not be held liable for data loss incurred by the user/party concerned because of unauthorised use of his/her Lifepassport ID. The user/party concerned may not use the personal codes assigned to him/her by Lifepassport without the express permission and consent of the holder of such codes. Meshpass shall not be liable for any loss or damage arising from failure to comply with these obligations.

The user/party concerned may review and edit his/her profile information at any time. Through certain features of the Service, the user/party concerned may also make some information public by sharing his/her Private Card and Medical Card codes, as well as the activation code. Once the univocal nature of the input code to access the WHH system is recognised, the Lifepassport service will share information in the system with the holder of the codes unless the user/party concerned promptly informs us not to do so using the blocking service. Indeed, in particular, the Medical Card, because of the nature of the service offered by Lifepassport, will always have access to the WHH if the entered code corresponds and has not previously been inhibited by the user/party concerned and owner.

Public information may be disclosed rapidly on a large scale, we therefore invite the holder to block codes as soon as possible in the event of theft, loss or other similar event.

Where the data is incorrect, we shall try to provide the user/party concerned with ways to quickly update or delete them, unless we are obliged to keep them for legitimate legal reasons. In the

event of updating of personal information, we may ask the user/party concerned to verify his/her identity before fulfilling his/her requests.

Relationship between the user/party concerned, LifpassportPRO and health professionals

Meshpass does not enter into relationships between user/parties concerned and health professionals, and therefore is not responsible for the processing of data and information carried out by LifepassportPRO users. The users/parties concerned are aware that by authorising health professionals to access their data via LifepassportPRO the latter are authorised to process or qualify the same as the data controller.

Service providers, business partners and others
Meshpass may use some companies and individual reliable third parties to help provide, analyse and improve the Service. This may include, for example, data storage, maintenance services, database management, analytical data on the web, the processing of payments, answering client questions about products and services and improving the functionality of the service.

Meshpass shall only provide such companies with personal information, and never medical/health information, that need to know in order to provide the Service, such as the IP or email address but never medical and health data. Meshpass requires companies to keep information confidential and prohibits them from using it for any other purpose. In fact, such third parties may have access to information of the user/party concerned to be able to perform activities respecting obligations similar to those contained in this Privacy Policy.

Our Website may contain links to other websites of independent third parties ("Linked Sites") such as health centres authorised by the user/party concerned and banks. These linked sites are provided solely for the convenience of our visitors. These linked sites are not under the control of Meshpass, and therefore Meshpass shall not responsible for and does not endorse the content of such linked sites, including any information or materials contained therein.

Meshpass may refuse requests that are unreasonably repetitive, require disproportionate technical effort (for example the development of a new system or substantial change of an existing practice), jeopardize the privacy of others or those that are impracticable (e.g. requests for information stored on backup tapes). Where possible, Meshpass allows access to information and its correction, without payment, unless if it is unduly burdensome. Meshpass tries to manage its services in a manner that protects information from accidental or unlawful destruction. For this reason, after a user user/party concerned has removed information from its services, Meshpass may not immediately eliminate the remaining copies from its active servers and may not remove information immediately from its backup systems.

Third-party applications
If the user user/party concerned decides to access Lifepassport using third-party applications, the same shall ensure that these applications have security protocols and a privacy policy. If the characteristics related to privacy and security of these applications do not satisfy the user user/party concerned, the same should not use them to access Lifepassport. For example, third-party applications may not use encryption in data transmission, may collect information that Lifepassport does not collect or use the information in a manner that is different from Lifepassport.

Meshpass may share the information of the user/party concerned with third parties with his/her consent, for example when decides to access our Service through this application. Meshpass shall not be responsible for the processing of information by these parties, so the user ensure that

he/she is confident about the use of an application and that the relevant privacy policies are acceptable.

In order to access the Service, the navigation Browser must provide the user user/party concerned with accurate information about the practices adopted with regard to privacy and compliance with applicable laws. Meshpass may revoke access to the Service to a browser if the program in question does not meet the undertakings made in the privacy area. However, Meshpass neither controls nor monitors these programs, if not to restrict access to Programmes to Lifepassport data, and the practices regarding privacy vary. The user should contact Meshpass if he/she believes that a program is not protecting the privacy or security of health data.

Compliance with laws and demands of law enforcement bodies; Protection of the Rights of Meshpass

We may disclose the files of the user/party concerned to parties except Meshpass, as well as information we have acquired except for medical and health data when we believe in good faith that such disclosure is reasonably necessary to (a) comply with laws, regulations or binding legal requests; (B) protect any person from death or serious bodily injury; (c) prevent fraud or abuse to the detriment of Meshpass or its users; or (d) protect the rights or property of Meshpass; (e) receive payments from the user/party concerned. In the event that Lifepassport user user/party concerned files are handed-over to the police for the above-mentioned reasons, we will remove the encryption from the files before delivery. However, Meshpass will not be able to decrypt any files encrypted by users before being stored in Lifepassport.

Any such disclosure request regarding medical data must be sufficiently substantiated and documented and Meshpass shall only comply if expressly and formally required by investigating authorities.

Business unit sale

In the event of a merger, acquisition or sale of all or part of our company, information regarding users may be transferred as part of these transactions. Users shall in any case be notified (e.g. via email and/or through a prominent notice on our Website) of any changes in the control and the use of personal information or files of the user/party concerned if they are affected by a different Privacy Policy. Users shall also be warned of the possible choices regarding the information.

Non-private or non-personal Information and the newsletter

Information that is not private, aggregated or that is non-personal information in any other manner, such as statistics on the use of our Service, may be disclosed.

The statistical functionality of the Lifepassport application collects all necessary and relevant data in order to produce unbiased, reliable, appropriate, timely, consistent and accessible statistics. Where appropriate, the statistics conform to the standards, guidelines and good practices agreed by Switzerland, European Union countries and on an international level. Under the principle of "statistical confidentiality", Meshpass ensures the protection of confidential statistical data that relates to individual statistical units and is collected directly from WHH holders. Confidential statistical information shall not be used for purposes other than purely statistical ones. Under the provisions of the Law (Federal Law on Data Protection) this data is treated confidentially.

The use of e-mail can involve substantial risks such as lack of confidentiality, potential manipulation of contents or sender's address, wrong recipients, viruses etc. Thus, Meshpass

expressly disclaims any liability for damages arising from the use of e-mail. Lifepassport therefore recommends not sending sensitive information, not to attach response received text replies and the manual entering of e-mails each time a message is sent.

The user user/party concerned gives his/her consent to the storage and processing of personal data by Meshpass in accordance with privacy regulations for individual information, for marketing purposes and to receive periodic newsletters. The user may, at any time, access the area dedicated to their personal data and revoke his/her consent to regular newsletters.

4. Modification or Deletion of Data belonging to the user/party concerned

Registered users may review, update, correct or modify personal information provided during registration or in their account. If the information that can personally identify a user user/party concerned undergoes changes or the user user/party concerned no longer wishes to use our service, the same may update or delete it by changing the settings of his/her account. In some cases we may retain a copy of the information, if required by law. For questions regarding your personal information on our service, please contact support@lifepassport.org. We will reply to your requests within 30 days.

5. Storage of Data Abroad

Personal and health information stored via the Service may be transferred and processed in Switzerland (home server) and/or at other destinations outside the European Economic Area ("EEA") or any other country in which Meshpass SA, its subsidiaries, affiliates or service providers are based. If the user user/party concerned has used an address located in the European Economic Area during the registration process, the health records thus created are stored in Switzerland, or SEE or in countries in relation to which the European Commission has granted “Adequacy decisions”.

Meshpass may retain data until the deactivation of an account or as long as is necessary to provide the services. If the user wishes to delete his/her account or request that his/her information not be used to provide other services, the user may order us to delete the data from his/her account. We may retain and use the user’s information as necessary to comply with our legal obligations, resolve disputes and enforce contracts. In accordance with these requirements, we will try to promptly delete the information upon request.

All data entered by the user shall only be accessible by the data controller or its delegates in possession of the appropriate authorisation codes, in complaince with the privacy code.

6. Security

The security of the user’s information is important to Meshpass. When the user enters sensitive data, we encrypt the transmission of that information using secure socket layer technology (SSL).

We follow generally accepted standards to protect information sent to us. However, no method of transmission or electronic storage is 100% safe. However, we cannot guarantee the security of data transmitted to this website; all transmissions are at the user’s own risk.

7. Regulations in respect of minors

The use of the Lifepassport service is only allowed to people over 16 years of age (we define users under this age minors in respect of these rules).

All individuals considered minors may access the Lifepassport service solely subject to parental authority.

All data and content entered in Lifepassport shall only be entered under the responsibility of an adult and never by any underage Lifepassport user. Without going into specific detail, leaving full power to entitled parties, the Medical Card shall be made available to minors who can view or ask others to display Lifepassport data issued by their parents, while the Private Card shall not be made available to minors to avoid any kind of interference on loadable data.

8. The User's Rights

We hereby inform you that you may exercise the rights recognised by the cited article at any time by contacting Meshpass SA, the data controller.

In particular, the user may exercise the following rights:

- ask us not to process his/her personal data for marketing purposes;
- receive information in regard to which personal data is subject to processing and what the processing methods consist in;
- request the correction or deletion of his/her personal data or at any time or withdraw his/her consent to data processing.

The user may also exercise the right to have the data deleted, i.e. request the total cancellation of his/her with immediate effect. Deletion is normally immediate from when the user enables the deletion procedure but, to allow us to delete data that is also in backup devices, we can take up to 2 months to ensure complete deletion of data form all devices, from the date deletion or service renewal is requested.

9. Contacts and Lifepassport Service Subscribers

In case of any doubt concerning this Privacy Policy and/or if the user wishes to exercise his/her rights, he/she can send a request to the following email address: privacy@lifepassport.org.

10. Amendment to our privacy regulations

This Privacy Policy may be changed periodically.

Meshpass may make changes to this privacy policy by notifying the user/party in question. Meshpass may send alerts about changes in other circumstances. The user shall be deemed to agree to be bound by the new privacy policy by continuing to access or use the Services after the changes come into force. In such a case, the date of the last update indicated in the initial part of the privacy statement shall also change. We recommend periodically reviewing this privacy statement in order to always be aware of the initiatives taken by Meshpass to protect the confidentiality of personal data it has collected. The user's continued use of the Service is deemed to be consent to this privacy statement and any updates.

11. Additional information

11.1 The registered office of Meshpass SA is in Switzerland, Corso Elvezia 13, IDI N.CHE-318.333.508.

11.2 The processing of personal data of the user/party shall be based on principles of correctness, lawfulness and transparency, protecting your privacy, rights and in accordance with the corporate privacy policy. The company also undertakes to process data in compliance with the principle of "minimization", in other words acquiring and processing data to the extent necessary with respect to the purpose of providing the service, statistical surveys, collection of payments, marketing and legal protection;

11.3 We process the following data:

11.3.1 For your information, the personal and sensitive data of users such as health data: diseases, medical procedures, examinations, hospitalizations, family history, allergies, vaccinations, drug therapies, infectious and mental diseases, DNA structure, images diagnostics etc. religious convictions, ethical choices. The purpose is only the provision of the service and, in anonymous format, statistical surveys. The recipients are only the user/party or their delegates and the recipient is Meshpas for the statistical surveys;

11.3.2 personal data: name, company name, email address, residence, location, telephone numbers, gender, etc. The purpose is the provision of the service and statistical surveys. The recipients are the user/party, the latter's delegates, those responsible for legal matters in the event of non-compliance with contractual obligations or fraud;

11.3.3 financial data: bank account details, credit card data, payment instruments. The purpose is the provision of the service. The recipients are banks and financial operators.

11.4 We only process data if the party has given his/her consent.

11.5 The Data Controller undertakes to rely exclusively on parties who provide adequate guarantees regarding data protection, and will appoint them as Data Processors. The list of Data Processors is available from the company and the party may view it upon request to the Data Controller.

11.6 Medical data shall not be disseminated.

11.7 At any time, the party concerned may exercise, in relation to the data controller, the rights prescribed by the current regulations. In particular, at this moment, the party concerned may have the right to ask for:

- access to one's own personal data;
- rectification in case of incorrectness of data;
- deletion;
- processing limitation.

Additional and specific information pursuant to EU Privacy Law 2016/679 for European users

12.1 Meshpass had adopted an organisational model regarding the protection of personal data in relation to the new GDPR (EU Privacy Code 2016/679)

12.2 The Eurpean Commission has established, on the basis of Article 45 of EU Regulation 2016/679 that the level of protection provided by **SWITZERLAND** is adequate (Adequacy decisions) and thatis therefore possible to transfer personal data there.

12.3 Rights to the provision of information (article 13 GDPR):

1. Data collected from parties concerned

a) Data controller: **Meshpass SA** with registered office in Switzerland, Corso Elvezia 13, IDI N.CHE-318.333.508 email: support@lifepassport.org

b) For all matters concerning the processing of data and the exercise of rights under the Regulation, the user can contact the Data Protection Officer at the following email address: privacy@lifepassport.org

c) The data is processed solely for the purpose of providing the Lifepassport service and, in an anonymous format, for statistical and research activities;

d) the legitimate interest of the Data Controller is included in the Lifepassport service offer;

e) user data is solely processed by the Data Controller and its delegates;

f) The data is processed in Switzerland. It is also possible that it may be processed in the European Economic Area or in countries for which the European Commission has granted "Adequacy decisions".

2. Additional information

a) The data is kept for the period strictly necessary for the provision of the service. In case of cancellation of the service for any reason, the data will be promptly deleted within 2 months from the moment in which the service is canceled.

b) The user can directly modify or delete his/her personal data. The user can oppose the processing of data at any time by terminating the service.

d) The user can lodge a complaint with the competent supervisory authority in the country in question:

e) The communication of the user's personal data is left to the free initiative of the same;

f) The automated decision-making processes, where applicable, are aimed at the execution of the contract between Meshpass and the user;

3. Meshpass does not process personal data for purposes other than those contractually provided for without informing the user in advance;

12.4 Data not collected by the party concerned (article 14 GDPR): The data recorded by Meshpass made available to the user/party concerned or health professionals authorised by the former via the LifepassportPRO platform or information systems platform. Meshpass does not collect data form health professionals who have not been authorised by the party concerned in advanced. Meshpass identifies the Data Controller and the latter's representative, where applicable. Data that is not collected from the user/party concerned is processed according to the same rules as those applicable to data collected from the party concerned.

12.5 Right of access of the party concerned (article 15 GDPR): For the type of service, the data collected by Meshpass is made available to the user or authorised health professionals.

12.6 The right of rectification (article 16 GDPR). The user has the possibility of rectifying or integrating his/her incomplete personal data.

12.7 The right to deletion ("right to obscurity") (article 17 GDPR). The user has the right to directly delete personal data concerning him/her.

12.8 Right to data portability (Article 20 GDPR) The user has the right to data portability for the period in which the service is active by downloading annexes and extracting his/her own “Patient summary dataset”.

12.9 Right of opposition (article 21 GDPR). The user has the right to object to the processing of data by withdrawing from the service and activating the automatic deletion function regarding all the data. This procedure is irreversible.

12.10 The right to communication of personal data violation (article 34 GDPR). Meshpass informs the user, via email, of each access to its platform and notifies the user of the violation of personal data that may present a high risk the user of his/her rights and liberties.

Meshpass Sa