GDPR Statement from the CEO of Medisanté to all our customers.

How prepared is Medisanté for GDPR?

We have acted and will continue to act on many fronts to adhere to these regulations to protect your rights. We have raised awareness across the organization through frequent internal discussions and trained all employees to handle systems and data appropriately.

Everyone working for Medisanté understands the importance of information security and the high standards currently being set by GDPR, EDPB and related CJEU rulings such as Schrems II. We have assessed against the aforementioned references the systems of Medisanté, the ones of our service providers, as well as M+ Hub, our vendor-agnostic telehealth device cloud. We have taken actions to ensure better management of data and will maintain a continuous ongoing assessment of the relevant standards, rulings, and guidelines.

We offer a Data Processing Agreement (DPA) that includes information on the role of Medisanté as a data processor for M+ Hub, our vendor-agnostic telehealth device cloud. The DPA details the various categories of data processed, access rights, storage conditions as well as all our processes and procedures, including a Data Retention Policy. M+ hub does neither manage nor process (de-identify/anonymise) personal data from patients. It only processes and manages names and email addresses of Users as detailed in the DPA terms agreed with the Users' employer. These Users are typically technical stakeholders such as health IT engineers or biomedical engineers who are in charge of device interoperability with their health IT system and device management of their fleet in remote patient monitoring (RPM) or decentralized clinical trials (DCT).

M+ Hub is a non-device Medical Device Data System (MDDS) that was designed to eliminate the inherent risk of exposing patient data when using a mobile app from a device manufacturer to send device readings to a target health IT system via a proprietary cloud. By abstracting in a single cloud (M+ Hub) a broad range of OEM devices (M+ ready devices) that connect direct2cloud, Medisanté redefines device interoperability and management in virtual care while shielding care teams and their patients from device complexity and privacy concerns:

- in M+ Hub, technical stakeholders of our clients can seamlessly and securely connect M+ ready devices with their compliant target health IT-system. Medisanté and the manufacturers of our M+ ready devices never have access to any patient ID or patient identifiable information that is held in such a target system; a multi-year joint R&D effort allowed us to eliminate the need for the patient to unveil any information in a mobile app in order to transmit device readings. Instead, care teams assign a device to a patient directly in their compliant health IT system and the readings get transmitted direct2cloud to M+ Hub, from where they get pushed automatically to the target health IT system. The format and authentication methods at reception in the target system are chosen by its technical stakeholders who are Users within M+ Hub. Encryption and other security protocols from device to cloud as well as in the telehealth device cloud itself are key elements to protect the device readings from source to destination.

- in M+ Hub, they can also manage though a single pane of glass M+ ready devices across vendor, platform, country, and organizational silos in order to reduce the operational costs of device deployment. The device data is void of personal patient data. It includes static device inventory data, as well as dynamic physiological (blood pressure, blood glucose, …) and device health (battery level, signal strength, …) readings. As a key tenet of the overall architecture, the management console is the one that keeps the mapping between a device ID, all its readings, and a target health IT system. The logs with the physiological readings are accessible only to a limited number of key developers at Medisanté in order to maintain and improve the platform.

Version: 2.0 Dated: 24.11.2021
Approved by Gilles Lunzenfichter
Released by Manuel Stocker

Beyond the unique focus on privacy and security within M+ Hub, we have taken the following company level initiatives to protect your privacy:

- We have assessed our sub-processors (third party service providers) and our contracts with them to ensure that they have addressed the pressing needs of the current security and developing privacy requirements specifically around the Schrems II ruling and EDPB recommendations.

- We have a dedicated Data Protection Officer and our developers have embraced the concept of privacy by design and have provided you more control over the data stored in our systems. We constantly endeavour to provide you with more enhancements.

- We conducted internal audits and risk analysis of our products, processes, operations, and management. The findings were communicated to our teams who have worked out the solutions to improve our data security methods and processes. This includes e.g., ensuring encryption of data at rest and protecting/limiting access to both cloud and physical assets based on the level of sensitivity and the likelihood of risks.

- When needed, breach notifications will be made within 72 hours after Medisanté becomes aware of it. For incidents specific to an individual user or an organization, we will notify the concerned party through email (using their primary email address).

- We have revised our Privacy Policy and Terms of Service to incorporate the requirements of the applicable privacy laws based on our data inventory, data flows, and data handling practices.

As a global innovator in medical IoT, Medisanté:

- received the global connected health trailblazer award for chairing the direct2cloud IoT activity workgroup in the Personal Connected Health Alliance (PCHA) in 2019. This work directly contributed to the extension of the Continua Guidelines to direct2cloud connectivity.

- is featured as the global partner of Thales in device interoperability with virtual care platforms on their Internet of Medical Things website. This cooperation helps to build a medical IoT world in which we all can trust.

- leverages the global technologies of partners such as AWS, Vodafone, and Thales for non - identifiable device data while leaving the entire data sovereignty of sensitive patient data to compliant health IT systems with a track record of protecting the privacy of their patients and meeting specific regulatory requirements in healthcare and life science.

Yours sincerely.

CEO, Medisanté Group AG

APPROVAL SECTION

Medisanté Group AG

Name: Gilles Lunzenfichter	Name: Manuel Stocker
Title: Chief Executive Officer	Title: Data Protection Officer
Signature: 	Signature: 
Date signed: 24.11.2021	Date signed: 24.11.2021