



Last update – December 2025

PRIVACY POLICY

ARTICLE 1: PREAMBLE

The protection of the Personal Data is paramount to Dental Monitoring SAS (“**DM**”). DM undertakes to comply with French and European regulations on the protection of personal data, in particular the General Data Protection Regulation (EU) of April 27, 2016 (“**GDPR**”), la Loi Informatique et Libertés de 1978 as amended (“**LIL**”), as well as any applicable local data protection regulation to the Processing.

In order to comply to GDPR and local data protection regulations as HIPAA and protect the confidentiality, integrity and availability of the Personal Data, including the Data Concerning Health (“**Data Concerning Health**”) as the Protected Health Information (“**PHI**”), DM has developed and implemented strong cybersecurity standards, policies, procedures and trainings to its employees, and also, strong security safeguards.

DM has a team dedicated to the protection of Personal Data, including a Data Protection and HIPAA Officer, a security team and a legal team specialized in privacy aspects.

In addition, please bear in mind that DM has ISO 13485 (Medical Device Quality Management System), ISO/IEC 27001 (Information Security) and HDS/HDH (Health Data Host) certifications. In addition, the Personal Data of Healthcare Professionals and Patients are hosted on local AWS’ servers (ISO27001 & HDS/HDH certified), under Dental Monitoring’s responsibility.

ARTICLE 2: DEFINITIONS

Capitalized terms set out below, including those in the preamble of the Privacy Policy, shall have the following meaning:

Data Protection Law: means (i) the EU General Data Protection Regulation 2016/679 (“**GDPR**”), (ii) the e-Privacy Directive 2002/58/EC (“**e-Privacy Directive**”), and any further applicable legislation replacing the e-Privacy Directive and/or the GDPR; (iii) any data protection law, statute or regulation of a European Union (“**EU**”) Member State, which may apply to one of the Parties pursuant to its data Processing activities or its establishment within the EU and (iv) any guidelines or opinion adopted by the European Data Protection Board (“**EDPB**”) as to interpret the application of GDPR and the e-Privacy Directive (v) the decisions of the Supervisory Authority or the judicial or administrative courts of an EU Member State which are binding on one of the Parties by way of its data Processing activities or its establishment within the EU; and (vi) the decisions rulings adopted by the Court of Justice of the European Union (CJEU) or the European Court of Human Rights (ECHR) regarding Personal Data and privacy protection and freedom of speech or freedom of information; and (vii) any applicable local data protection regulation to the processing, including, for example, HIPAA or Federal and state or territory laws, such as but not limited to Personal Information Protection and Electronic Documents Act (“**PIPEDA**”), Personal Information Protection Act (Alberta) (“**PIPA Alberta**”), Personal Information Protection Act (British Columbia) (“**PIPA BC**”) and An Act Respecting the Protection of Personal Information in the Private Sector (“**Quebec Privacy Act**”) for Canadian citizens

“**Controller**”, “**Processing**” and “**Supervisory Authority**” shall have the meaning assigned to them in Article 4 of the GDPR.



Dashboard: means the web-based interface for authenticated Healthcare Professionals reachable after creating an HCP Account, on the DM Platform.

TOU: means these terms and conditions of use.

DM Mobile Application: refers to the DM App.

DM Platform: refers to the DM Platform.

DM Software Products and Services: refers to DentalMonitoring, Engage, Smart STL described in the TOU and offered by DM through the DM Platform and DM Mobile Application.

DM Hardware Products: refers to DM Scanbox, DM Cheek Retractors and Scanbox Pro and Led Adapter.

DM Solution: refers to the software, digital infrastructures, protocols, interfaces, mobile applications and hardware developed, manufactured and distributed by DM for use in the dental health sector.

End User(s) or Patient(s): means the patient(s) who is/are browsing the DM Software Products and Services.

Data concerning health : shall have the meaning assigned to them in Article 4 of GDPR, including the the PHI;

Healthcare Professional(s) or HCP: means the natural person's health provider(s) qualified to practice dentistry or orthodontics in their jurisdiction.

Patient Account: refers to the End User's account created by the HCP on DentalMonitoring or by Patients or by the HCP, to gain access to the DM App and, therefore, to the DM Software Products and Services.

Personal Data: shall have the meaning assigned to them in Article 4 of GDPR, including the Data Concerning Health and, therefore, the PHI.

Privacy Policy: refers to the privacy policy available on the DM Platforms and DM Mobile Applications dedicated to inform Users and End Users of the commitments taken by DM to protect Users' and End Users' Personal Data when they use the DM Software Products and Services.

Protected Health Information or PHI: means information, including demographic information, that relates to (i) a past, present, or future physical or mental health or condition; (ii) the past, present, or future provision of health care; or (iii) the past, present, or future payment for the provision of health care; and (2) identifies the person who is the subject of the information or with respect to which there is a reasonable basis to believe the information can be used to identify such person. Protected Health Information is limited to the covered entity's information created or received by DM from or on behalf of the Client or the covered entity.

Purposes: refers to the main purposes of the use of Personal Data.

Stripe: Refers to the platform dedicated to online payments used by DM to manage payments made by Users on the DM Platform through the HCP Shop.

You/Your: You designate.



ARTICLE 3. WHAT IS PERSONAL DATA?

A Personal Data means any information relating to an identified or identifiable natural person (“**Data subject**”). A Data Subject is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

ARTICLE 4. WHAT IS THE PURPOSE OF THIS PRIVACY POLICY ?

This Privacy Policy explains:

- how DM collects, uses and shares Your Personal Data when you use the DM Software Products and Services and the DM Hardware Products;
- how DM protects and ensures the security, integrity and confidentiality of your

Personal Data. DM follows these principles in order to protect Your Personal Data:

- DM does not collect any more Personal Data than is necessary;
- DM only uses your Personal Data for the purposes specified in this Privacy Policy, unless you agree otherwise;
- DM does not keep your Personal Data if it is no longer needed; and
- Other than as we specify in this Privacy Policy, DM does not share your Personal Data with third parties.
- DM does not rent or sell your Personal Data to third parties.

Whether you are a Healthcare Professional or a Patient, please take the time to read and understand this Privacy Policy.

ARTICLE 5. WHO COLLECTS PERSONAL DATA?

HCP data	Patient data
DM acts as sole Controller for Processing n°1 to n°6 described in Section 7 of this Privacy Policy. As an exception, when contracting with public organizations or entities (such as hospitals) : DM may act as a Processor for Processing n°1, described in Section 7 of this Privacy Policy. DM may act as a Sole Controller for Processing n°2 to n°6 described in Section 7 of this Privacy Policy.	DM acts as Joint Controller with HCP (when HCP is self-employed) or with HCP’s employer (when HCP is employed by a company) for the Processing n°1 described in Section 7 of this Privacy Policy. DM acts as sole Controller for Processing n°2 to n°6 described in Section 7 of this Privacy Policy. As an exception, when contracting with public organizations or entities (such as hospitals) : DM may act as a Processor for Processing n°1, described in Section 7 of this Privacy Policy.



	DM may act as a Sole Controller for Processing n°2 to n°6 described in Section 7 of this Privacy Policy.
--	--

DM and Stripe act as Joint Controllers for the Processing n°3 in Section 7 of this Privacy Policy regarding both HCPs and Patients.

Please bear in mind that for any other Personal Data collected or processed by the HCPs during the course of the Patients' treatment and that are not shared with DM, the HCPs will remain solely and fully responsible for compliance with applicable laws and regulations.



ARTICLE 6. WHAT PERSONAL DATA IS COLLECTED ?

DM collects Personal Data from both HCPs and Patients.

FROM HEALTHCARE PROFESSIONALS

The HCPs' Personal Data processed by DM are collected through different channels.

DM collects HCPs' personal data when they sign up to one of the DM Software Products and Services.

DM may collect the following Personal Data when a HCP signs up to one of the DM Software Products and Services:

Account data	• Account credentials (user id, email, password hash); • The HCP's personal information (first and last name, phone number, email address); • User settings (newsletter preferences, language, protocols, notification settings, country).
---------------------	--

DM may collect the following Personal Data when a HCP uses one of the DM Software Products and Services:

Technical data	• Device information (type of device, IP address, unique identifier, device model, operating system and version, browser used, cookies or similar technologies, system language); • Information about usage of the DM Software Products and Services (IP address, connection date and time, pages visited); • Data about the internet connection (internet service provider, connection type (4G, 3G, DSL).
Usage data	• User activity logs; • Messages sent to Patients; • Appointments booked with Patients; • Account configurations (email templates, dental notation preferences, treatments catalogs, protocols).

DM may collect the following Personal Data when a HCP contacts customer support:

Support ticket data	• Details regarding support tickets (date, time, subject and content of tickets) • Content of exchanges with agents (emails, chat) • Any other data that may be necessary to resolve tickets
----------------------------	--



DM may collect the following Personal Data when a HCP subscribes to the DM Software Products and Services or purchases DM Hardware Products:

Subscription data / order data	• Invoices, credit notes, and other administrative documents; • Transaction details (payment method, transaction date and time, currency, amount paid); • Contact information (first name, last name, email, phone number); • Shipping address (street, city, postal code, country); • Order details.
---------------------------------------	---

FROM THE PATIENTS

DM collects Personal Data from the Patients when they are registered to one of the DM Software Products and Services.

DM collects Personal Data from Patients after gathering their consent through a Patient consent form. If the patient is under the age of majority in its country of residence, the consent is managed by their legal guardian(s), except if they're emancipated minors. Please take time to read and understand our Terms of Use to obtain more information.

Patients' Personal Data processed by DM is collected through different channels.

Personal Data may either be collected directly from Patients, or indirectly by HCPs. In the case where a HCP enters a Patient's Personal Data into one of the DM Software Products and Services on the Patient's behalf, the HCP is responsible for ensuring it is legally allowed to do so and that the necessary measures have been taken with regards to applicable laws and regulations.

DM may collect the following Personal Data when a Patient registers to use one of the DM Software Products and Services:

Account data	• Account credentials (user ID, email, password hash); • Personal and contact information (first and last name, phone number, email address, profile picture (picture of the face), date of birth, legal representative when applicable, the name of private practice where the patient receives treatment at, postal address); • User settings (protocols, notification settings).
---------------------	---



DM may collect the following personal data when Patients use one of the DM Software Products and Services:

Technical data	• Device information (type of device, IP address, unique identifier, device model, operating system and version, browser used, cookies or similar technologies, system language); • Information about usage of the software (IP address, connection date and time, pages visited); • Data about the internet connection (internet service provider, connection type (4G, 3G, DSL).
Usage data	• Messages sent to the HCP; • Appointments booked with the HCP; • User preferences;
Health data	• Pictures of the Patient's mouth; • Profile picture (picture of the face); • Medical treatment and/or advice prescribed by the HCP; • Treatment type and phase; • Screening / analysis / simulation results; • Messages exchanges between the HCP and the Patient containing medical data such as symptoms, reasons to consult and general health information; • Digital impression of the Patient's mouth.

DM may collect the following Personal Data when Patients contacts the customer support service:

Support ticket data	• Details regarding the support ticket (date, time, subject and content of your ticket); • Content of the Patient's exchanges with DM's staff (emails, chat); • Any other data that may be necessary to resolve the ticket.
----------------------------	---

DM may collect the following Personal Data when a Patient purchases directly DM Hardware Products, following their HCP recommendations, already being a DM user:

Order data	• Contact information (first name, last name, email, phone number); • Shipping address (street, city, postal code, country); • Order details.
-------------------	---

ARTICLE 7. WHY AND HOW DO WE PROCESS YOUR PERSONAL DATA ?

DM processes Personal Data as part of multiple Processing and for multiple purposes. Depending on the purposes, Processing can be based on (i) the legitimate interests pursued by DM, (ii) on contractual obligations, or (iii) because you gave your consent.

For your information, please note the Processing listed below describes the main purpose and then the sub-purposes.



CONCERNING HEALTHCARE PROFESSIONALS

DM processes HCPs' Personal Data for the following Purposes and based on the following legal basis:

PROCESSING n°1: MAIN PURPOSE IS TO DELIVER THE DM SOFTWARE PRODUCTS AND SERVICES (MONITORING, ENGAGE, SMART STL)	
Sub-purposes	Legal Basis
To set up, configure and manage HCPs' accounts (for MONITORING and ENGAGE)	Processing n°1 is necessary for the performance of a contract to which the HCP (Data Subject) is party (Article 6.1 (b) of GDPR)
To enable HCP to remotely monitor their Patients' orthodontic treatment and oral health (only for MONITORING)	
To provide HCP with assessments of their Patients' oral and dental health (only for ENGAGE)	
To enable HCPs to provide their Patients with simulations of their appearance during and after orthodontic treatment (only for ENGAGE)	
To generate smart STL Files (3D object files computed from a Scan and STLs files, an initial intra-oral scan and from the treatment plan of an End User) and manufacture aligners (only for SMART STL)	
PROCESSING n°2: MAIN PURPOSE IS TO MANAGE HCPs' TICKETS (FEEDBACK/COMPLAINTS/QUESTIONS) WITH CUSTOMER SUPPORT SERVICES FOR ALL DM SOFTWARE PRODUCTS AND SERVICES	
Sub-purposes	Legal Basis
To manage the feedback, complaints and issues from HCPs including by sending messages to the HPCs (SMS, whatsapp, email, notification)	Processing n°2 is necessary for the performance of a contract to which the HCP (Data Subject) is party (Article 6.1 (b) of GDPR) or fulfill its legal obligations (Article 6.1 (c) of GDPR) such as transfer data privacy requests
To transfer the data privacy request to the privacy team	
To improve the quality and the speed of the customer care that DM provides to HCPs and their Patients	
PROCESSING n°3: MAIN PURPOSE IS TO MANAGE HCPs' PAYMENTS AND SHIPPING ORDERS FROM THE DM SOFTWARE PRODUCTS AND SERVICE AND HARDWARE PRODUCTS	
Sub-purposes	Legal Basis



To process payments when HCPs subscribe to the Software Products and Services or purchase Hardware Products	Processing n°3 is necessary for the performance of a contract to which the HCP (Data Subject) is party (Article 6.1 (b) of GDPR) or fulfill its legal obligations (Article 6.1 (c) of GDPR) such as fiscal law and regulations.
To proceed with the shipping of orders	
To fulfill DM's accounting and legal obligations	
PROCESSING n°4: MAIN PURPOSE IS TO IMPROVE AND MONITOR THE DM SOFTWARE PRODUCTS AND SERVICES AND HARDWARE PRODUCTS	
Sub-purposes	Legal Basis
To improve the DM Software Products and Services and develop new features	Processing n°4 is based on the DM's legitimate interest in improving healthcare service quality (Article 6.1 (F) of GDPR)
To send surveys to HCPs to gather experience and optimize the DM Software Products and Services	
PROCESSING n°5: MAIN PURPOSE IS TO SECURE THE DM SOFTWARE PRODUCTS AND SERVICES AND THE DM HARDWARE PRODUCTS	
Sub-purposes	Legal Basis
To ensure the security, confidentiality, integrity and availability of the DM Software Products and Services	Processing n°5 is based on the DM's legitimate interest in improving healthcare service quality and comply with Data Protection Laws (Article 6.1. (F) of GDPR)
PROCESSING n°6 : MAIN PURPOSE IS TO IMPROVE THE RELATIONSHIP WITH THE HCP	
Sub-purposes	Legal Basis
To maintain a good business relationship with HCPs by organizing contests, loyalty program, sponsorship, grant discounts to HCPs	Processing n°6 is based on the DM's legitimate interest in improving healthcare service quality and comply with Data Protection Laws (Article 6.1. (F) of GDPR)

PATIENT DATA

DM processes Patients' Personal Data for the following purposes and based on the following legal basis:

PROCESSING n°1: MAIN PURPOSE IS TO DELIVER THE DM SOFTWARE PRODUCTS AND SERVICES (MONITORING, ENGAGE, SMART STL)	
Sub-purposes	Legal Basis
To set up and manage Patients' accounts (only for MONITORING and ENGAGE)	Processing n°1 is necessary for the performance of a contract to which the HCP (Data Subject) is party (Article 6.1 (b) of GDPR) and on the explicit consent of the Patient which is gathered by the reading and the acceptance of the Patient consent form (Art. 9.2 2) (a) of GDPR) <i>Please note that when contracting with public organizations or entities (such as hospitals), DM relies on patient consent to process the Patients' personal data, public organizations supervising Patient treatments may not rely on consent but on 'public task' in compliance with specific and local privacy regulations.</i>
To contact by phone or send messages (by SMS, whatsapp, email or notifications) to the Patients on their HCP's behalf to remind them to send their scans (<u>AI based processing for the notifications if HCPs decide to use AI communication tools to communicate with their patients</u>) (only for MONITORING)	
To enable HCP to remotely monitor their Patient's orthodontic treatment and oral health and assist their decision making process with regards to their Patients' treatment, to provide analytical support and optimize treatment outcomes (<u>AI based processing</u>) (only for MONITORING)	
To provide HCP and Patients with an assessment of: - teeth health - gum health - teeth alignment (<u>AI based processing</u>) (only for ENGAGE)	
PROCESSING n°2: MAIN PURPOSE IS TO MANAGE PATIENTS' TICKETS (FEEDBACK/COMPLAINTS/QUESTIONS) WITH CUSTOMER SUPPORT SERVICES FOR ALL DM SOFTWARE PRODUCTS AND SERVICES	
Sub-purposes	Legal Basis
To manage the feedback, complaint and issue from Patients	Processing n°2 is necessary for the performance of a contract to which the HCP (Data Subject) is party (Article 6.1 (b) of GDPR) or fulfill its legal obligations (Article 6.1 (c) of GDPR) such as transfer data privacy requests
To transfer the data privacy request to the privacy team	
To improve the quality and the speed of the customer care DM provides to Patients	

PROCESSING n°3: MAIN PURPOSE IS TO IMPROVE AND MONITOR THE DM SOFTWARE PRODUCTS AND SERVICES AND HARDWARE PRODUCTS	
Sub-purposes	Legal Basis
To improve the DM Software Products and Services and develop new features, to train AI systems for internal improvement purposes (AI based processing)	Processing n°3 is based on the DM's legitimate interest in improving healthcare service quality (Article 6.1 (F) of GDPR) and / or on the explicit consent of the Patient which is gathered by the reading and the acceptance of the Patient consent form (Art. 9.2 2) (a) of GDPR)
To send surveys to Patients to gather experience and optimize the DM Products and Services	
To do some statistics or studies on the performance of the DM Products and Services (clinical studies are not included here) to optimize the DM Products and Services (such statistics are based on patients data but generating aggregated results and data relating to HCPs' use of the DM Products and Services excluding personal data)	
PROCESSING n°4: MAIN PURPOSE IS TO ILLUSTRATE PATIENTS' CASES IN PRESENTATIONS OR ON DEMO ACCOUNTS	
Sub-purposes	Legal Basis
To illustrate webinar, presentation of DM's Software Products and Services (only on a case by case basis and when appropriate to illustrate specific cases, not for all Patients in general)	Processing n°4 is based on the Patient's explicit consent and on the DM's legitimate interest in improving healthcare service quality (Article 6.1 (F) of GDPR)
PROCESSING n°5: MAIN PURPOSE IS TO SECURE THE DM SOFTWARE PRODUCTS AND SERVICES AND DM HARDWARE PRODUCTS	
Sub-purposes	Legal Basis
To ensure the security, confidentiality, integrity and availability of the DM Software Products and Services	Processing n°5 is based on the DM's legitimate interest to process in improving healthcare service quality and comply with Data Protection Laws (Article 6.1. (F) of GDPR)

AI-Based Processing

Some personal data (including health data) may be processed using Artificial Intelligence (“AI”) systems to support treatment monitoring, improve service accuracy, and assist HCPs as described in the list of processing above (see processing n°1 and n°3 for patients). These AI systems are designed to assist HCPs by providing automated insights or recommendations based on data collected for Patients’ remote dental treatments, orthodontic treatments, and oral health check up.

The results generated by DM Software Products and Services are intended to be used as an aid in diagnosis to support the clinical judgment of qualified dental professionals and not on a stand-alone basis for clinical decision-making.

ARTICLE 8: HOW DO WE SHARE PERSONAL DATA ?

Internal use: Personal Data of the HCPs and Patients may be processed by the employees of DM (within the limits of their respective attributions and only on a need to know basis) and its subsidiaries and group companies, exclusively in order to achieve the purposes of this Privacy Policy.

External use: DM may share Personal Data (only if appropriate and to the extent permitted by the applicable laws) with the following categories of third parties:

HEALTHCARE PROFESSIONALS’ DATA

Technical suppliers	● Cloud services and storage suppliers (AWS) ● Networking and telecommunication suppliers ● Maintenance suppliers ● Security services suppliers ● Property Management Systems suppliers (if applicable)
Payment processors	● Credit card payment processor (Stripe) ● Direct debit payment processor (GoCardless) ● DM’s banks
External vendors used by HCPs	● Aligners manufacturers and PMS service providers used by the HCPs
Marketing suppliers	● Customer relationship management software ● Marketing automation software
Authorities	● Legal, judicial and administrative authorities

PATIENTS' DATA

Technical suppliers	• Cloud services and storage suppliers (AWS) • Networking and telecommunication suppliers • Maintenance suppliers • Security services suppliers
Payment processors	• Credit card payment processor (Stripe)
External vendors used by HCPs	• Aligners manufacturers and PMS service providers used by the HCPs
Authorities	• Legal, judicial and administrative authorities

DM ensures data transfers to these parties are secured by following a strict ISO 27001 compliant process to verify they have the necessary organizational and technical measures to comply with relevant data protection legal requirements, security standards and quality standards.

Some of these third parties may be located abroad or may host the Patient's data abroad. For these specific cross-border data transfers, DM has set up specific data privacy contractual clauses to ensure that these third parties apply protective measures to the Patient's Personal Data that respect the Patient's country's legal requirements.

ARTICLE 9. WHERE DO WE STORE YOUR PERSONAL DATA?

The Software Products and Services are hosted in Amazon Web Service Inc (AWS) cloud services, with servers in different locations around the world in order to locally store Personal Data in Europe, US, Japan and APAC depending on the location of residence of Patients and HCPs.

AWS' servers are ISO 27001 and HDS/HDH compliant and Personal Data storage location is compliant with regulation in each country where DM operates.

ARTICLE 10. HOW LONG DO WE STORE YOUR PERSONAL DATA?

DM processes and stores both HCP's and Patient's Personal Data for the duration required by the purposes for which it is collected and in compliance with applicable laws and regulations.

ARTICLE 11. WHICH ARE YOUR DATA PROTECTION RIGHTS? HOW CAN YOU EXERCISE YOUR RIGHTS?

Data Protection Laws give rights to European citizens with regards to their Personal Data. GDPR being globally considered as the reference standard in personal data protection matters, DM enables its users across the world to benefit from these rights (some of these rights may be limited by applicable local laws and regulations in certain circumstances), which are:

- **A right to access**, as the right to obtain from the Controller, as to whether or not Personal Data concerning You are being processed, and, where that is the case, access to the Personal Data and the following information, including, the purposes of the Processing, the categories of Personal Data concerned, the recipients or categories of recipient to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organizations etc.
- **A Right to obtain the rectification**, without undue delay, of inaccurate, incomplete, outdated Personal Data concerning you, or whose the collect is forbidden;

-
- **A Right to oppose** before to a Personal Data Processing realized by the Controller or to a Personal Data transfer, except if there are legitimate and compelling reasons that prevail on your interests;
 - **Right to obtain from the Controller the erasure of Your Personal Data** undue delay and the Controller shall have the obligation to erase Personal Data without undue delay where one of the following grounds applies:
 - The Personal Data are no longer necessary in relation to the Purposes;
 - You withdraw the consent on which the Processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the Processing;
 - You object to the Processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing or DM objects to the Processing pursuant to Article 21(2);
 - The Personal Data have been unlawfully processed;
 - The Personal Data have to be erased for compliance with a legal obligation in Union or Member State law to which the Controller is subject;
 - The Personal Data have been collected in relation to the offer of information society services referred to in Article 8(1).
 - **Right to Personal Data portability**, i.e. the right to receive Your Personal Data which You have provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the personal data have been provided, where:
 - (a) The Processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
 - b) The Processing is carried out by automated means.
 - **Right to object and request information about automated individual decision-making (AI).**

You may request information about whether and how AI systems have processed your data. You have the right to obtain meaningful information about the logic involved and the potential consequences of such processing. You may request human intervention or review of any AI-assisted outcome that concerns you.

- **Right to lodge a complaint before the Supervisory Authority**, if you consider that the Processing of the Personal Data that You concerned are a violation of the Data Protection Laws.

For any complaint, you may submit a complaint to the national supervisory authority ("**Supervisory Authority**") responsible for the protection of personal data, namely the National Commission for Data Protection and Liberties (the "**CNIL**") for example in France.

Other citizens, including US citizens, can refer to the laws of their jurisdiction to find more information on their rights and the Supervisory Authority. As examples:

- HIPAA and any other state and territory laws relating to Privacy for the US citizens;
- Federal Privacy Act 1988 and any other state and territory laws, such as but not limited to : Information Privacy Act 2014 (Australian Capital Territory), Information Act 2002 (Northern Territory), Privacy and Personal Information Protection Act 1998 (New South Wales), Information Privacy Act 2009 (Queensland), Personal Information Protection Act 2004 (Tasmania) and Privacy and Data Protection Act 2014 (Victoria)for Australian citizens;

-
- Federal and state or territory laws, such as but not limited to Personal Information Protection and Electronic Documents Act (PIPEDA), Personal Information Protection Act (Alberta) (PIPA Alberta), Personal Information Protection Act (British Columbia) (PIPA BC) and An Act Respecting the Protection of Personal Information in the Private Sector (Quebec Privacy Act) for Canadian citizens.
 - the UK GDPR and the Data Protection Laws for UK citizens. Etc.

To exercise any of your rights, you can send a request:

- By email at the following address: privacy@dental-monitoring.com .
- By letter at the following postal address: Data Protection Officer - Dental Monitoring SAS, 75 rue de Tocqueville, 75017 Paris, France

In the event that you exercise one of your rights electronically, the Personal Data will be provided, where appropriate, electronically by DM where possible, except that You have specifically requested that it is otherwise.

HCPs and Patients should specify the nature of their request in the email's subject and specify the details of the request in the email itself. DM may request additional information from the HCP or Patient, in order to verify their identity, before moving forward with the request.

ARTICLE 12. HOW YOUR PERSONAL DATA IS PROTECTED AND SECURED?

DM has taken steps so that HCPs and Patients can rest assured their Personal Data is safe when using the DM Software Products and Services and more generally when their Personal Data is processed by DM.

Technical, organizational and structural security measures are in place to protect Your Personal Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction and, therefore, ensure the security, integrity and confidentiality of Your Personal Data.

DM develops its systems under the "Privacy by Design" principles.

We also follow data minimization principles and set up the following measures:

- Pseudonymization and anonymization techniques whenever they are technically feasible; and
- Restricting Personal Data access to the sole employees who need to access Personal Data to perform the services described in the Service description, ensured by a regular review of access rights performed by the IT department.

We have implemented state-of-the-art IT security measures to protect your Personal Data and regularly perform penetration tests to detect any vulnerability incident.

In case of incident , DM will investigate the incident and conduct a risk assessment to determine our course of action moving forwards. DM has implemented a dedicated policy referring to a specific procedure for handling events relating to Personal Data.

Depending on the results of this assessment, DM we will take all necessary and required measures and actions to comply with applicable laws and regulations which may include notifying impacted users in the likelihood of a higher risk to their rights and freedom, notifying the Supervisory Authorities if necessary etc.

ARTICLE 13. CAN THE PRIVACY POLICY BE UPDATED?

DM may update the Privacy Policy from time to time and will notify HCPs and Patients of significant changes in the way we treat any Personal Data by disclosing a notice. We encourage you to periodically review this page for the latest information on our privacy practices.