



隱私權政策

第 1 條:前言

個人資料的保護對 Dental Monitoring SAS(以下簡稱「DM」)至關重要。DM 承諾遵守法國及歐洲關於個人資料保護的法規,特別是 2016 年 4 月 27 日的《歐盟一般資料保護規則》(以下簡稱「GDPR」)、經修訂的 1978 年《資訊技術、資料文件及個人自由法》(以下簡稱「LIL」),以及任何適用於資料處理的當地資料保護法規。

為遵守 GDPR 以及如 HIPAA 等當地資料保護法規,並保護個人資料(包括健康相關資料 [下稱「健康相關資料」],作為受保護健康資訊 [下稱「PHI」])的機密性、完整性與可用性,DM 已制定並實施了嚴格的網路安全標準、政策、程序及員工訓練,還有強大的安全防護措施。

DM 擁有一個專責保護個人資料的團隊,包括一名資料保護與 HIPAA 合規官、一個安全團隊以及一個專精於隱私事務的法律團隊。

另請知悉,DM 已獲得 ISO 13485(醫療器材品質管理系統)、ISO/IEC 27001(資訊安全)以及 HDS/HDH(健康資料託管)認證。同時,健康護理專業人員與患者的個人資料皆託管於當地 AWS 的伺服器(通過 ISO27001 與 HDS/HDH 認證),並由 Dental Monitoring 負責管理。

第 2 條:定義

本隱私權政策中使用的以下術語,包括前言中的術語,應具有下列涵義:

資料保護法:係指 (i)《歐盟一般資料保護規則》2016/679(「GDPR」);(ii)《電子隱私指令》2002/58/EC(「電子隱私指令」),以及任何後續取代電子隱私指令及/或 GDPR 之適用法律;(iii) 歐盟(「EU」)成員國之任何資料保護法律、法令或規章,其可能因某一方的資料處理活動或機構位於歐盟境內而適用於該方;以及 (iv) 歐洲資料保護委員會(「EDPB」)所通過的關於如何解讀 GDPR 及電子隱私指令應用的任何指引或意見;(v) 因某一方的資料處理活動或機構位於歐盟境內而對該方具有約束力之歐盟成員國監管機關或者司法或行政法院決議;以及 (vi) 歐盟法院(CJEU)或歐洲人權法院(ECHR)就個人資料與隱私保護以及言論自由或資訊自由而通過的決議裁決;以及 (vii) 任何適用於資料處理之當地資料保護法規,包括但不限於 HIPAA 或聯邦和州或領地法律,例如(針對加拿大公民)《個人資訊保護與電子文件法》(「PIPEDA」)、《亞伯達省個人資訊保護法》(「亞伯達省 PIPA」)、《不列顛哥倫比亞省個人資訊保護法》(「不列顛哥倫比亞省 PIPA」)以及《私營部門個人資訊保護法》(「魁北克隱私法」)

「控制者」、「處理」及「監管機關」應具有 GDPR 第 4 條賦予其之涵義。

儀表板:係指於 DM 平台上建立 HCP 帳戶後,經身分驗證的健康護理專業人員可存取的網頁介面。

TOU:係指這些使用條款與條件。

DM 行動應用程式:係指 DM 應用程式。

DM 平台:係指 DM 平台;

DM 軟體產品與服務:係指 TOU 中所述的、由 DM 透過 DM 平台與 DM 行動應用程式提供的



DentalMonitoring、Engage、Smart STL。

DM 硬體產品：係指 DM ScanBox、DM 牽引器、ScanBox Pro 以及 Led 配接器。

DM 解決方案：係指由 DM 開發、製造和分銷的供口腔健康機構使用的軟體、數位基礎設施、協定、介面、行動應用程式及硬體。

終端使用者或患者：係指正在瀏覽 DM 軟體產品與服務的患者。

健康相關資料：應具有 GDPR 第 4 條賦予其的含義，包括 PHI；

健康護理專業人員或 HCP：係指在其司法管轄區內具備牙科或矯正科執業資格的自然人醫療服務提供者。

患者帳戶：係指由 DentalMonitoring HCP 或由患者或由 HCP 建立的終端使用者帳戶，用於存取 DM 應用程式，以便使用 DM 軟體產品與服務。

個人資料：應具有 GDPR 第 4 條賦予其的含義，包括健康相關資料，因此也包括 PHI。

隱私權政策：係指在 DM 平台與 DM 行動應用程式上公告之隱私權政策，旨在告知使用者與終端使用者，當他們使用 DM 軟體產品與服務時，DM 為保護使用者及終端使用者個人資料而做出的承諾。

受保護健康資訊或 PHI：係指包含人口統計資料在內的資訊，這些資訊關係到 (i) 過去、現在或未來的身體或心理健康或狀況；(ii) 過去、現在或未來的醫療保健服務提供；或 (iii) 過去、現在或未來的醫療保健費用支付；且能夠識別資訊所屬的個人，或有合理依據令人相信這些資訊可用於識別該個人。受保護健康資訊僅限於以客戶或受管轄實體為來源或作為客戶或受管轄實體的代表，DM 建立或接收的、歸屬於受管轄實體的資訊。

目的：係指使用個人資料的主要目的。

Stripe：係一個線上支付專用平台，DM 使用該平台來管理使用者在 DM 平台上透過 HCP 商店進行的交易付款。

您/你們：指代您。



第 3 條:什麼是個人資料?

個人資料係指任何與已識別或可識別之自然人(「資料當事人」)相關的資訊。資料當事人是指可直接或間接識別之自然人,特別是透過姓名、身分識別號碼、位置資料、線上識別碼等識別符,或透過與該自然人之身體、生理、遺傳、心理、經濟、文化或社會特徵相關的一項或多項特定因素來識別。

第 4 條:本隱私權政策之目的為何?

本隱私權政策旨在說明:

- 當您使用 DM 軟體產品與服務以及 DM 硬體產品時, DM 如何收集、使用及分享您的個人資料;

- DM 如何保護並確保您個人資料的安全性、完整性及機密性。DM 遵循以下原則

來保護您的個人資料:

- DM 僅收集必要範圍內的個人資料;
- 除非您另行同意, DM 僅會將您的個人資料用於本隱私權政策中說明的目的;
- 若不再需要您的個人資料, DM 將不會保留;且
- 除本隱私權政策中明確說明的範圍外, DM 不會與第三方分享您的個人資料。
- DM 不會將您的個人資料出租或出售給第三方。

無論您是健康護理專業人員還是患者,請花時間閱讀並理解本隱私權政策。

第 5 條:誰收集個人資料?

HCP 資料	患者資料
對於本隱私權政策第 7 部分所述的資料處理 1 至 6, DM 作為單獨控制者。 例外情況:當與公共組織或實體(例如醫院)簽約時: 對於本隱私權政策第 7 部分所述的資料處理 1, DM 可能作為處理者。 對於本隱私權政策第 7 部分所述的資料處理 2 至 6, DM 可能作為單獨控制者。	對於本隱私權政策第 7 部分所述的資料處理 1, DM 與 HCP(當 HCP 為自僱人士時)或 HCP 的僱主(當 HCP 受僱於公司時)作為聯合控制者。 對於本隱私權政策第 7 部分所述的資料處理 2 至 6, DM 作為單獨控制者。 例外情況:當與公共組織或實體(例如醫院)簽約時:對於本隱私權政策第 7 部分所述的資料處理 1, DM 可能作為處理者。 對於本隱私權政策第 7 部分所述的資料處理 2 至 6, DM 可能作為單獨控制者。

對於本隱私權政策第 7 部分中的資料處理 3, 無論是涉及 HCP 還是患者, DM 均與 Stripe 作為聯合控制者。



請注意，對於 HCP 在患者治療過程中收集或處理的未與 DM 共享的任何其他個人資料，HCP 將仍單獨並完全負責遵守適用的法律和法規。



第 6 條: 收集哪些個人資料?

DM 會同時向 HCP 和患者收集個人資料。

向健康護理專業人員收集個人資料

DM 所處理的 HCP 個人資料是透過不同途徑收集的。

當 HCP 註冊任一 DM 軟體產品與服務時, DM 會收集其個人資料。

當 HCP 註冊任一 DM 軟體產品與服務時, DM 可能會收集以下個人資料:

帳戶資料	● 帳戶憑證(使用者 ID、電子郵件、密碼雜湊); ● HCP 的個人資訊(姓名、電話號碼、電子郵件地址); ● 使用者設定(新聞通訊喜好設定、語言、協定、通知設定、國家/地區)。
------	--

當 HCP 使用任一 DM 軟體產品與服務時, DM 可能會收集以下個人資料:

技術資料	● 裝置資訊(裝置類型、IP 位址、唯一識別碼、裝置型號、作業系統及版本、使用的瀏覽器、Cookie 或類似技術、系統語言); ● 關於 DM 軟體產品與服務使用情況的資訊(IP 位址、連線日期與時間、瀏覽的頁面); ● 關於網際網路連線的資料(網際網路服務供應商、連線類型 [4G、3G、DSL])。
使用情況資料	● 使用者活動日誌; ● 傳送給患者的訊息; ● 與患者預約的就診; ● 帳戶設定(電子郵件模板、牙位表示法喜好設定、治療目錄、協定)。

HCP 聯絡客戶支援時, DM 可能會收集以下個人資料:

支援工單資料	● 關於支援工單的詳細資訊(工單的日期、時間、主題及內容) ● 與客服人員溝通的內容(電子郵件、聊天記錄) ● 為處理工單所必需的任何其他資料
--------	---



當 HCP 訂閱 DM 軟體產品與服務或購買 DM 硬體產品時，DM 可能會收集以下個人資料：

訂閱資料/ 訂單資料	● 發票、貸項通知單及其他行政文件； ● 交易明細(付款方式、交易日期與時間、幣別、支付金額)； ● 聯絡資訊(名字、姓氏、電子郵件、電話號碼)； ● 送貨地址(街道、城市、郵遞區號、國家/地區)； ● 訂單詳細資料。
---------------	---

向患者收集個人資料

當患者註冊任一 DM 軟體產品與服務時，DM 會向患者收集個人資料。

DM 在透過患者同意書取得患者的同意後，才收集其個人資料。若患者未達其居住地的法定成年年齡，則應由其法定監護人代為作出同意，獨立未成年人除外。請花時間閱讀並理解我們的使用條款以獲取更多資訊。

DM 所處理的患者個人資料是透過不同途徑收集的。

個人資料可能直接向患者收集，或間接透過 HCP 收集。若 HCP 代表患者將其個人資料輸入任一 DM 軟體產品與服務中，該 HCP 有責任確保該行為合法，並且已根據適用法律和法規採取必要措施。

當患者註冊使用任一 DM 軟體產品與服務時，DM 可能會收集以下個人資料：

帳戶資料	● 帳戶憑證(使用者 ID、電子郵件、密碼雜湊)； ● 個人與聯絡資訊(姓名、電話號碼、電子郵件地址、個人頭像(臉部照片)、出生日期、法定代理人(若適用)、患者就醫之私人診所名稱、郵寄地址)； ● 使用者設定(協定、通知設定)。
------	--



當患者使用任一 DM 軟體產品與服務時，DM 可能會收集以下個人資料：

技術資料	● 裝置資訊(裝置類型、IP 位址、唯一識別碼、裝置型號、作業系統及版本、使用的瀏覽器、Cookie 或類似技術、系統語言)； ● 關於軟體使用情況的資訊(IP 位址、連線日期與時間、瀏覽的頁面)； ● 關於網際網路連線的資料(網際網路服務供應商、連線類型 [4G、3G、DSL])。
使用情況資料	● 傳送給 HCP 的訊息； ● 與 HCP 預約的就診； ● 使用者喜好設定；
健康資料	● 患者口腔的照片； ● 個人頭像(臉部照片)； ● 由 HCP 開立的治療及/或醫囑； ● 治療類型與階段； ● 篩檢/分析/模擬結果； ● HCP 與患者之間的訊息交流，包含醫療資料，例如症狀、就診原因及一般健康資訊； ● 患者口腔的數位印模。

當患者聯絡客戶支援服務時，DM 可能會收集以下個人資料：

支援工單資料	● 關於支援工單的詳細資訊(您的工單日期、時間、主題及內容)； ● 患者與 DM 工作人員的溝通內容(電子郵件、聊天記錄)； ● 為處理工單所必需的任何其他資料。
--------	---

當患者在成為 DM 使用者後根據其 HCP 的建議直接購買 DM 硬體產品時，DM 可能會收集以下個人資料：

訂單資料	● 聯絡資訊(名字、姓氏、電子郵件、電話號碼)； ● 送貨地址(街道、城市、郵遞區號、國家/地區)； ● 訂單詳細資料。
------	--

第 7 條: 我們為何及如何處理您的個人資料？

DM 會在多項資料處理中基於多種目的處理個人資料。依據目的之不同，資料處理的依據可能為：(i) 基於 DM 所追求的合法權益、(ii) 基於合約義務，或 (iii) 因為您已給予同意。

謹此告知，下表將列出各項資料處理，其中先說明主要目的，接著說明次要目的。



涉及健康護理專業人員

DM 出於以下目的、基於下列法律依據處理 HCP 的個人資料：

資料處理 1: 主要目的是提供 DM 軟體產品與服務 (MONITORING、ENGAGE、SMART STL)	
次要目的	法律依據
建立、設定及管理 HCP 的帳戶 (適用於 MONITORING 和 ENGAGE)	資料處理 1 對於履行 HCP (資料當事人) 作為一方當事人的合約是必需的 (GDPR 第 6.1 (b) 條)
使 HCP 能夠遠端監測其患者的矯正治療及口腔健康 (僅適用於 MONITORING)	
為 HCP 提供患者口腔及牙齒健康評估 (僅適用於 ENGAGE)	
使 HCP 能夠為其患者提供矯正治療期間及治療後的外觀模擬 (僅適用於 ENGAGE)	
生成 smart STL 檔案 (根據掃描檔和 STL 檔案、初始口內掃描以及終端使用者的治療計劃計算出的 3D 物體檔案) 並製造牙套 (僅適用於 SMART STL)	
資料處理 2: 主要目的是管理 HCP 就所有 DM 軟體產品與服務向客戶支援服務部提交的工單 (回饋/投訴/問題)	
次要目的	法律依據
管理來自 HCP 的回饋、投訴與問題, 包括透過向 HCP 傳送訊息 (簡訊、WhatsApp、電子郵件、通知) 進行管理	資料處理 2 對於履行 HCP (資料當事人) 作為一方當事人的合約是必需的 (GDPR 第 6.1 (b) 條), 或是為了履行法定義務 (GDPR 第 6.1 (c) 條), 例如轉交資料隱私請求
將資料隱私請求轉交給隱私團隊	
提升 DM 為 HCP 及其患者提供的客戶服務品質與速度	
資料處理 3: 主要目的是管理 DM 軟體產品與服務及硬體產品的 HCP 付款與裝貨單	
次要目的	法律依據



在 HCP 訂閱軟體產品與服務或購買硬體產品時處理付款	資料處理 3 對於履行 HCP(資料當事人)作為一方當事人的合約是必需的(GDPR 第 6.1 (b) 條), 或是為了履行法定義務(GDPR 第 6.1 (c) 條), 例如財政法及相關法規。
進行訂單出貨	
履行 DM 的會計與法律義務	
資料處理 4: 主要目的是改進與監測 DM 軟體產品與服務及硬體產品	
次要目的	法律依據
改進 DM 軟體產品與服務並開發新功能	資料處理 4 基於 DM 改進醫療服務品質之合法權益(GDPR 第 6.1 (F) 條)
向 HCP 傳送調查問卷以收集使用體驗, 並優化 DM 軟體產品與服務	
資料處理 5: 主要目的是保護 DM 軟體產品與服務及 DM 硬體產品的安全	
次要目的	法律依據
確保 DM 軟體產品與服務的安全性、機密性、完整性及可用性	資料處理 5 基於 DM 改進醫療服務品質之合法權益及旨在遵守資料保護法(GDPR 第 6.1 (F) 條)
資料處理 6: 主要目的是改善與 HCP 的關係	
次要目的	法律依據
透過組織競賽、忠誠計劃、贊助活動、為 HCP 提供折扣, 與 HCP 維持良好的商業關係	資料處理 6 基於 DM 改進醫療服務品質之合法權益及旨在遵守資料保護法(GDPR 第 6.1 (F) 條)

患者資料

DM 出於以下目的、基於下列法律依據處理患者的個人資料：

資料處理 1: 主要目的是提供 DM 軟體產品與服務 (MONITORING、ENGAGE、SMART STL)	
次要目的	法律依據
建立及管理患者的帳戶 (僅適用於 MONITORING 和 ENGAGE)	資料處理 1 對於履行 HCP (資料當事人) 作為一方當事人的合約是必需的 (GDPR 第 6.1 (b) 條), 並且基於患者透過閱讀及接受患者同意書而作出的明確同意 (GDPR 第 9.2) (a) 條) 請注意, 當與公共組織或實體 (例如醫院) 簽約時, DM 依賴患者同意來處理患者的個人資料, 而負責監督患者治療的公共組織可能不依賴同意, 而是依據如特定當地隱私法規所規定的「公共任務」。
代表 HCP 透過電話聯絡或傳送訊息 (簡訊、WhatsApp、電子郵件或通知) 給患者, 提醒他們傳送掃描檔 (若 HCP 決定使用 AI 通訊工具與患者溝通, 則相關通知推送涉及 AI 處理) (僅適用於 MONITORING)	
使 HCP 能夠遠端監測其患者的矯正治療及口腔健康, 協助其完成患者治療決策過程, 提供分析支援並優化治療結果 (AI 處理) (僅適用於 MONITORING)	
為 HCP 及患者提供以下評估: - 牙齒健康 - 牙齦健康 - 牙齒排列 (AI 處理) (僅適用於 ENGAGE)	
資料處理 2: 主要目的是管理患者就所有 DM 軟體產品與服務向客戶支援服務部提交的工單 (回饋/投訴/問題)	
次要目的	法律依據
管理來自患者的回饋、投訴與問題	資料處理 2 對於履行 HCP (資料當事人) 作為一方當事人的合約是必需的 (GDPR 第 6.1 (b) 條), 或是為了履行法定義務 (GDPR 第 6.1 (c) 條), 例如轉交資料隱私請求
將資料隱私請求轉交給隱私團隊	
提升 DM 為患者提供的客戶服務品質與速度	
資料處理 3: 主要目的是改進與監測 DM 軟體產品與服務及硬體產品	
次要目的	法律依據
改進 DM 軟體產品與服務並開發新功能, 出於內部改進目的訓練 AI 系統 (AI 處理)	資料處理 3 基於 DM 改進醫療服務品質之合法權益 (GDPR 第 6.1 (F) 條), 和/或基於

向患者傳送調查問卷以收集使用體驗，並優化 DM 產品與服務	患者透過閱讀及接受患者同意書而作出的明確同意 (GDPR 第 9.2) (a) 條)
對 DM 產品與服務的效能進行統計或研究 (不包括臨床研究)，以優化 DM 產品與服務 (此類統計基於患者資料，但會產生與 HCP 使用 DM 產品及服務相關的匯總結果和資料 [不包含個人資料])	
資料處理 4: 主要目的是在簡報或示範帳戶中展示患者病例	
次要目的	法律依據
在網路研討會、DM 軟體產品與服務簡報中進行病例展示 (僅進行逐個病例展示，且僅在適合進行具體病例展示時才展示，而非進行總體患者的概括性展示)	資料處理 4 基於患者的明確同意以及基於 DM 改進醫療服務品質之合法權益 (GDPR 第 6.1 (F) 條)
資料處理 5: 主要目的是保護 DM 軟體產品與服務及 DM 硬體產品的安全	
次要目的	法律依據
確保 DM 軟體產品與服務的安全性、機密性、完整性及可用性	資料處理 5 基於 DM 為改進醫療服務品質而進行資料處理之合法權益及旨在遵守資料保護法 (GDPR 第 6.1 (F) 條)

AI 處理

可能會使用人工智慧(「AI」)系統處理部分個人資料(包含健康資料)，以支援治療監測、提升服務準確性及協助 HCP，如上文的資料處理清單所述(請參閱患者資料處理 1 和 3)。這些 AI 系統經設計可根據為進行患者遠端牙科治療、矯正治療及口腔健康檢查而收集的資料，提供自動化見解或建議以協助 HCP。

由 DM 軟體產品與服務產生的結果用於輔助診斷，以支援合格牙科專業人士的臨床判斷，而非獨立用於臨床決策。

第 8 條:我們如何共享個人資料？

內部使用:DM 的員工(在其各自職權範圍內，且僅基於「僅知」原則)及其子公司和集團公司，可能僅為了實現本隱私權政策所述之目的而處理 HCP 和患者的個人資料。

外部使用:DM 可能會(僅在適當且符合適用法律的範圍內)與以下類別的第三方共享個人資料：

健康護理專業人員的資料

技術供應商	● 雲端服務與儲存供應商 (AWS) ● 網路與電信供應商 ● 維護供應商 ● 安全服務供應商 ● 物業管理系統 (PMS) 供應商(若適用)
支付處理商	● 信用卡支付處理商 (Stripe) ● 直接扣款支付處理商 (GoCardless) ● DM 的往來銀行
HCP 使用的外部供應商	● HCP 所使用的牙套製造商與 PMS 服務供應商
行銷供應商	● 客戶關係管理軟體 ● 行銷自動化軟體
主管機關	● 法律、司法及行政主管機關

患者資料

技術供應商	● 雲端服務與儲存供應商 (AWS) ● 網路與電信供應商 ● 維護供應商 ● 安全服務供應商
支付處理商	● 信用卡支付處理商 (Stripe)
HCP 使用的外部供應商	● HCP 所使用的牙套製造商與 PMS 服務供應商
主管機關	● 法律、司法及行政主管機關

DM 遵循符合 ISO 27001 的嚴格流程來確保將資料傳輸給以上各方是安全的，確認他們具備必要的組織與技術措施來遵守相關的資料保護法律要求、安全標準與品質標準。

部分第三方可能位於國外，或可能在國外託管患者的資料。針對這些特定的跨境資料傳輸，DM 已制定特定的資料隱私契約條款，以確保這些第三方對患者的個人資料實施符合患者所在國家/地區法律要求的保護措施。

第 9 條：我們將您的個人資料儲存在哪裡？

軟體產品與服務託管於 Amazon Web Service Inc (AWS) 的雲端服務中，其伺服器分佈於全球不同地點，以便依據患者與 HCP 的居住地將個人資料儲存在歐洲、美國、日本及亞太地區本地。

AWS 的伺服器符合 ISO 27001 及 HDS/HDH 規範，且個人資料的儲存地點均符合 DM 營運所在各個國家/地區的法規要求。

第 10 條：我們儲存您的個人資料多久？

DM 處理及儲存 HCP 與患者的個人資料之期限，是為達成資料收集目的所必需的時間，並遵守適用的法律和法規。

第 11 條：您擁有什麼資料保護權利？如何行使您的權利？

根據資料保護法律，歐洲公民對其個人資料擁有一些權利。鑑於 GDPR 在全球範圍內被視為個人資料保護事務的參考標準，DM 讓其全球使用者都能享有這些權利（在某些情況下，部分權利可能會受到當地適用法律和法規的限制），這些權利包括：

- 存取權：您有權向控制者確認與您相關的個人資料是否正在被處理，若情況屬實，您有權存取該個人資料及以下資訊，包括處理的目的、相關個人資料的類別、已獲得或將獲得資料的個人資料接收者或接收者類別（特別是第三國家/地區或國際組織內的接收者）等。
- 更正權：您有權要求毫不拖延地更正與您相關的不準確、不完整或過時的個人資料，或來自禁止收集對象的個人資料；
- 反對權：您有權在控制者進行個人資料處理或個人資料傳輸之前，反對這些處理或傳輸，除非存在優先於您利益的合法且令人信服之理由；
- 刪除權：您有權要求控制者毫不拖延地刪除您的個人資料，控制者有義務在以下任一理由成立時，毫不拖延地刪除個人資料：
 - 該個人資料對於實現目的已不再必要；
 - 您根據第 6(1) 條 (a) 點或第 9(2) 條 (a) 點撤回了資料處理所依據的同意

，且沒有其他法律依據來支援資料處理；

- 您根據第 21(1) 條反對處理，且不存在高於一切的合法處理理由，或者 DM 根據第 21(2) 條反對處理；
 - 個人資料被非法處理；
 - 為遵守控制者適用的歐盟或成員國法律中的法定義務而必須刪除個人資料；
 - 個人資料是為了提供第 8(1) 條所述的資訊社會服務而收集的。
- 資料可攜權：即在以下情況下，您有權以結構化、常用且機器可讀的格式，接收您提供給資料控制者的個人資料，並有權將這些資料傳輸給另一個控制者，而不受已獲得個人資料之控制者的阻礙：
 - (a) 資料處理是基於第 6(1) 條 (a) 點或第 9(2) 條 (a) 點所述的同意，或是基於第 6(1) 條 (b) 點所述的契約；且
 - (b) 資料處理是透過自動化方式執行的。
 - 反對個人化自動決策 (AI) 及獲取個人化自動決策相關資訊的權利：

您可以要求提供關於 AI 系統是否以及如何處理您的資料的資訊。您有權獲得關於此類處理所涉邏輯以及潛在後果的有意義資訊。您可以要求對任何與您相關的 AI 輔助結果進行人為干預或審查。

- 向監管機關提出投訴的權利：如果您認為對您關注的個人資料的處理違反了資料保護法律，您有權向監管機關提出投訴。

對於任何投訴，您可以向負責保護個人資料的國家/地區監管機關（「監管機關」）提出投訴，例如在法國即向國家資料保護與自由委員會（「CNIL」）提出投訴。

其他國家的公民（包括美國公民）可參考其司法管轄區的法律，以獲取有關其權利及監管機關的更多資訊。例如：

- 美國公民請參考 HIPAA 及與隱私相關的任何其他州和領地法律；
- 澳洲公民請參考《1988 年聯邦隱私法》及任何其他州和領地法律，例如但不限於：《2014 年資訊隱私法》（澳洲首都領地）、《2002 年資訊法》（北領地）、《1998 年隱私與個人資料保護法》（新南威爾斯州）、《2009 年資訊隱私法》（昆士蘭州）、《2004 年個人資料保護法》（塔斯馬尼亞州）以及《2014 年隱私與資料保護法》（維多利亞州）；
- 加拿大公民請參考聯邦及省或領地法律，例如但不限於：《個人資料保護與電子文件法》（PIPEDA）、《個人資料保護法》（亞伯達省）（亞伯達省 PIPA）、《個人資料保護法》（不列顛哥倫比亞省）（不列顛哥倫比亞省 PIPA）以及《私營部門個人資料保護法》（魁北克省隱私法）。
- 英國公民請參考英國 GDPR 及資料保護法律。等等。

若要行使您的任何權利，您可以透過以下方式傳送請求：

- 透過電子郵件傳送至以下地址：privacy@dental-monitoring.com。
- 透過信件寄至以下郵寄地址：Data Protection Officer - Dental Monitoring SAS,
75 rue de Tocqueville, 75017 Paris, France

若您以電子方式行使任一權利，DM 將在可能且適當的情況下以電子方式提供個人資料，除非您特別要求其他方式。

HCP 與患者應在電子郵件的主旨中說明其請求的性質，並在郵件正文中詳細說明請求的內容。DM 可能會在處理請求前，向 HCP 或患者索要額外資訊，以驗證其身分。

第 12 條：您的個人資料如何受到保護與確保安全？

DM 已採取相關措施，讓 HCP 與患者在使用 DM 軟體產品與服務時，以及在 DM 處理其個人資料的更廣泛情況下，能夠放心確信其個人資料是安全的。

我們已實施技術性、組織性與結構性的安全措施，以保護您的個人資料免於遭受意外、未經授權或非法的存取、洩漏、更改、遺失或銷毀，從而確保您個人資料的安全性、完整性與機密性。

DM 依據「隱私始於設計」原則來開發其系統。

我們還遵循資料最小化原則，並實施了以下措施：

- 在技術可行的情況下，採用假名化與匿名化技術；以及

- 限制個人資料的存取權限，即限定只有那些需要存取個人資料以執行服務說明中所述服務的員工才具有存取權限，由 IT 部門透過定期審查存取權限來確保這一點。

我們已實施最先進的 IT 安全措施來保護您的個人資料，並定期執行滲透測試以偵測任何安全漏洞事件。

若發生安全事件，DM 將調查該事件並進行風險評估，以決定我們後續的行動方針。DM 已實施專門的政策，其中指定了在處理與個人資料相關的事件時要遵循的特定程序。

根據此評估的結果，DM 將採取所有必要且必須的措施與行動，以遵守適用的法律與法規，這些措施與行動可能包括向權利與自由可能面臨較高風險的受影響使用者發出通知，以及在必要時向監管機關發出通知等。

第 13 條：隱私權政策是否可能更新？

DM 可能不時更新本隱私權政策，並將透過發佈公告的方式，通知 HCP 與患者我們在處理任何個人資料的方式上作出的重要變更。我們鼓勵您定期檢視此頁面，以獲取關於我們隱私權實務的最新資訊。