Vitalerter 維特爾公司 資訊安全政策

[最後更新：2018 年 9 月 18 日]

Vitalerter 維特爾公司 致力於提供其所實施的安全措施的透明度，以確保和保護我們為了提供其服務而處理的個人數據（定義見《歐盟通用數據保護條例》條例 2016/679 “GDPR”），詳細信息請參閱公司的隱私政策，網址為：privacy@vitalerter.com。

本資訊安全政策(“安全政策”）概述了公司截至上述 “最後更新” 日期所部署的當前安全措施。 我們將根據適用法律和我們內部政策的要求，不時更新本安全政策。 本文中的定義應具有 GDPR 或我們的隱私政策中規定的含義。

作為 GDPR 合規流程的一部分，我們實施了技術組織監控保護措施，並建立了廣泛的信息和網絡安全計劃，所有這些都與公司處理的個人數據有關。

系統訪問控制

只能通過公司的用戶身份驗證系統訪問所有數據處理系統。 只有一部分特定人員可以訪問系統。 對公司係統管理網絡的所有訪問都只能從辦公室通過專用暗光纖鏈接到數據中心進行。 對每個系統的身份驗證是通過用戶密碼進行的，該用戶密碼對於每個員工或人員來說都是唯一的，並且來自專用於此類環境的不同域控制器。系統對所有訪問系統的密碼做控制以及對手動操作做持續監控。

數據訪問控制

對個人數據的訪問僅限於需要訪問的員工。 員工接受有關個人數據安全的教育。

物理訪問控制

Vitalerter 維特爾公司 確保對存儲個人數據的數據服務器的物理訪問進行保護，並專門與 Microsoft Azure 配合使用，作為其託管個人數據的主要雲存儲（有關 Microsoft Azure 安全性的更多信息，請參閱此處 https://www.microsoft.com/en-us/trust-center/product-overview ）。

傳輸控制

傳輸控制的目標是確保個人數據在數據電子傳輸過程中或在傳輸到適用數據中心 (即 HTTPS) 的過程中不會被未經授權的各方讀取、複製、修改或刪除。 備份期間的數據傳輸是加密的。

可用性控制和目的控制

公司的服務器包含自動備份程序。 公司的備份概念包括每周自動備份。 執行定期檢查以確定備份是否已發生。

數據保留

個人數據以及原始數據將盡快或在法律要求的情況下盡快刪除，有關更多信息，請參閱我們的隱私政策：VITALERTER Privacy - Vitalerter **維特爾公司 GDPR 一般資料保護規範 合規性概述 文件**。

作業控制

員工和數據處理者都簽署了適用且具有約束力的協議，所有這些協議都包括適用的數據條款和數據安全義務，包括我們適用的合作夥伴。 員工有義務遵守公司的政策和程序，違規行為將受到紀律處分，嚴重者將被解僱。 除非公司相信員工受過良好教育並負責以安全的方式處理個人數據，否則員工將無法訪問個人數據。 公司已確保所有文件，包括但不限於協議、隱私政策在線條款等均符合 GDPR。 我們的法律團隊正忙於確保我們的法律文件得到更新，以反映任何變化並包含 GDPR 要求的強制性條款。 安全、法律、隱私和合規部門致力於確定適用於公司合規性的地區法律、法規。 因此，本安全政策可能會根據任何適用的立法或內部政策不時更新。

(英文正本如後續頁)

INFORMATION SECURITY POLICY

[Last Update: 18 September 2018]

Vitalerter Ltd. ("Vitalerter" or "Company" or "we") is committed to provide transparency regarding the security measures which it has implemented in order to secure and protect Personal Data (as defined under the EU General Data Protection Regulation (Regulation 2016/679) ("GDPR")) processed by the us for the purpose of providing its services as detailed in Company's Privacy Policy available at: privacy@vitalerter.com .

This information security policy ("Security Policy") outlines the Company's current security measures deployed by the Company as of the "Last Updated" date indicated above. We will keep updating this Security Policy from time to time, as required by applicable laws and our internal policies. Definitions herein shall have the meaning as set forth under the GDPR or in our Privacy Policy.

As part of our GDPR compliance process, we have implemented, technical organizational monitoring protections, and established an extensive information and cyber security program, all with regards to Personal Data processed by Company.

System Access Control

Access to all data processing systems is solely via Company's user authentication systems. Only a portion of specific personnel has access to systems. All access to Company's systems admin network are available solely from the office going through a private, dark fibre, link to the data centre. Authentication to each system is through a user-password, unique to each employee or personnel and from a different domain controller dedicated to such environment. Password control and manual and ongoing monitoring on all system access.

Data Access Control

The access to the Personal Data is restricted to solely the employees that are required to receive access. Employees are educated with regards to security of the Personal Data.

Physical Access Control

Vitalerter ensures the protection of the physical access to the data servers which store the Personal Data and works exclusively with Microsoft Azure, as its main cloud storage to host the Personal Data (for additional information regarding Microsoft Azure Security see here).

VITALERTER
A vital leap to quality patient care

Transfer Control

The goal of transfer control is to ensure that Personal Data cannot be read, copied, modified or removed by unauthorized parties during the electronic transmission of data or during their transport in motion, to the applicable data center (i.e., HTTPS). Transmission of data during backups is encrypted.

Availability Control and Purpose Control

The Company's servers include an automated backup procedure. The Company has a backup concept which includes automated weekly backups. Periodical checks are preformed to determine that the backup have occurred.

Data Retention

Personal Data as well as raw data are deleted as soon as possible or as soon as legally required, for more information please see our Privacy Policy available at: VITALERTER Privacy.

Job Control

Employees and data processors are all signed on applicable and binding agreements all of which include applicable data provisions and data security obligations, including our applicable Partners. Employees are bound to comply with the Company's policies and procedures and violations shall result in disciplinary actions up to and including termination of employment. An employee will not gain access to the Personal Data until the Company has trust that the employee is well educated and responsible to handle the Personal Data, in a secure manner. Company has ensured all documents, including without limitations, agreements, privacy policies online terms, etc. are compliant with the GDPR. Our Legal team is busy ensuring our legal documentation is updated to reflect any changes and to include the mandatory provisions required by the GDPR. The security, legal, privacy and compliance departments work to identify regional laws, regulations applicable to Company's compliance. Therefore, this Security Policy may be updated from time to time, according to any applicable legislation or internal policies.