



後 GDPR 時代資料 保護與網路安全



#KingstonIsWithYou

序言

無數的公司和組織都努力不懈且致力於招聘人才，以便為 GDPR 預作準備。也許您也是其中之一。然而，不斷演進的網路威脅本質代表您無法承受停下腳步並喘口氣所可能產生的損失。遵循 GDPR 並非逐項檢查的打勾練習，而是可用於判斷目前正在進行之資料保護與網路安全工作的架構。我們不因此而感到自滿。

在這本簡短的電子書中，我們彙總了英國一些經驗最豐富之網路安全評論員的知識，進而討論自引進 GDPR 之後，資料保護發生了何種變化。電子書內容也涵蓋公司如何對員工指導符合法規遵循性的需求，以及討論 IT 部門和技術提供者如何加強保護 IT 基礎架構並教導一般使用者如何因應新興的安全挑戰。



撰稿人

這本簡短的電子書由五位資料保護和網路安全專家撰寫。



Rob Allen
@Rob_A_kingston

Rob 是 Kingston Technology 行銷及技術服務部總監，而且自 1996 年便任職於此。Rob 的職掌範圍是監督利用 Digital Marketing Media and Creative，針對所有 Kingston 品牌及產品所進行的公關、社群媒體、頻道行銷效果。



Tara Taubman-Bassirian
@clarinette02

Tara 有很多頭銜：律師、辯護人、調解人、研究員、顧問、演講者和作家。她在隱私權、知識財產和資料保護等領域擁有令人讚嘆的專業知識，因此在世界各地頗具聲望，在英國、法國和美國等地最為知名。



Rafael Bloom
@rafibloom73

Rafael 是 Salvatore Ltd 的總監，負責協助公司管理因為技術和法規變更而產生的策略、商務及程序挑戰上帶來的機會。



Miriam Brown
@Kingston_MBrown

他是 Kingston Technology 的 B2B 策略行銷經理，自 1997 年便任職於此。Miriam 的工作職掌是為所有 Kingston B2B 產品規劃行銷策略、內容和宣傳活動。



Sally Eaves
@sallyeaves

Sally Eaves 教授向來被稱為道德技術的「啟蒙者」。作為新興技術領域的教授和全球策略顧問，她為執行長和技術長帶來豐富經驗。Sally 是屢獲殊榮的國際主講人、作家、研究員和影響者，可分享原始和真誠的思維領導力。

目錄

第一部分	採用 GDPR 以來，資料保護發生何種變化？	5 - 7
第二部分	機構如何教導員工？	8 - 9
第三部分	IT 部門能夠更妥善地保護裝置嗎？	10 - 11
第四部份	技術提供者如何改善流程和加強理解？	12 - 13
	摘要	14
	關於 Kingston	15



第一部分 - 採用 GDPR 以來， 資料保護發生何種變化？



公司經歷了大幅進展。在過去的兩年中，法律團隊編制擴大、資料保護專員的招聘人數激增¹，而且向外部資料隱私權顧問進行的諮詢也增加了。數以千計的組織現在對於完成資料保護影響評估 (DPIA) 已經很熟悉了。

但未來還有很長的路要走。

GDPR 面臨的最大挑戰之一就是您不能失去專注力。在大多數組織中，幾乎任何員工，在任何時候都可能違反規定。在需要大量勞力或是擁有高度自治權的領域 (例如，醫療、教育和法律)，這個問題更為嚴重。舉法律領域為例，許多律師都覺得透過簡單的電子郵件附

件來交換敏感案件的細節，是很稀鬆平常的事。醫療保健專業人員會透過不安全的電子郵件地址，交換患者資料或 MRI 掃描結果。在面臨高度壓力的組織中，只要對代辦事項清單增加一點額外的壓力，就可能超出法規遵循性的範圍。產能看似比協定更有用。

這點必須改變。

慈善部門的意識也有問題。慈善機構常常認為自己不受 GDPR 的約束。即使他們明白 GDPR 適用於每個私營、公共和第三領域組織，但他們並不情願 (這也是可以理解的) 將資金從企業營運轉為挹注資料保護之投資。

那種作法很偉大，但也很無知。與違反 GDPR 的潛在罰款相比，可能的 IT 支出顯得微不足道。



Tara Taubman-Bassirian
@clarinette02

GDPR、資料保護與 IP 顧問

「許多第三部門組織都認為：'GDPR 不適用於我們，我們只是慈善機構。即使在網站法規遵循性方面，我試著告訴他們，這與你們要收集的資料無關，而是與允許存取訪客資料的第三方有關。」

自 2016 年以來

對資料保護官 (DPO) 的需求
激增，增幅超過 700%。

1. Varonis：實施 GDPR 的一年：統計數據與要點須知
www.varonis.com/blog/gdpr-effect-review/ [存取時間：2019 年 11 月 26 日]

資料最少收集原則 (Data minimisation) 是令人鼓舞的趨勢

我們身處資料遭到異常收集的時代。「四巨頭」(Google、Apple、Facebook 及 Amazon) 持有巨量的客戶資料。其他組織可能會仿效「四巨頭」的作法，然後盡可能地收集資料。但是您持有的資料越多，所面臨的風險就越大。自推行 GDPR 以來，最正面的趨勢之一就是反對過度的資料收集。聰明的公司會採用資料最少收集原則：亦即，如果您不需要資料，就不要收集。



Tara Taubman-Bassirian
@clarinette02

GDPR、資料保護
和 IP 顧問

「資料最少收集原則可能是 GDPR 的最佳原則之一。任何資料庫的建立都意味著風險的產生。」



Rob Allen
@Rob_A_kingston

Kingston Technology
行銷與技術服務總監

「我們設有嚴格的資料刪除規則。是的，必須正確地儲存業務型關鍵資料。但還有其他的嗎？在一年後就消失了。持有資料的重點為何？」

好處影響範圍遠遠超越了限制風險。舉行銷為例。如果您的行銷資料庫「不衛生」，則表示您持有的可能是過時的資料。如果您的資料庫執行涉及到上萬人，而且您經常執行電子郵件宣傳活動，成本便會增加。這也會讓您的宣傳活動績效統計數據產生誤差。

資料最少收集原則也適用於實體資料。請留意您列印的內容(如客戶護照的掃描文件)；留意您寫下的內容(如帳戶密碼)。此外，如果需要留存某個東西的實體副本，請將之存放在安全位置。桌上堆疊成山的文件看起來可能很壯觀。但這並不安全。



Rafael Bloom
@rafibloom73

Salvatore Ltd
總監

「我們正在見證一種完全不同的方法，而能思考技術與業務實際營運之間的介面。需要極度努力，才能實現企業領導力之中的數位成熟度。」

接觸影響： 從高層主管到消費者

資料保護作為一種管制概念，已經存在了幾十年。但截至目前為止，Google¹、英國航空公司 (British Airways) 和萬豪連鎖酒店集團² 在內的公司已經被處以巨額罰款(以及因此而產生的媒體報導)，也已經引起高層主管對 GDPR 的關注。這也導致涓滴效應。

1. Varonis：實施 GDPR 的一年：統計數據與要點須知
www.varonis.com/blog/gdpr-effect-review/ [存取時間：2019 年 11 月 26 日]
2. 《衛報》：GDPR 罰款：英航和萬豪的三億英鎊將何去何從？
www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [存取時間：2019 年 11 月 26 日]

續下頁...

採用強大資料保護背後的另一個動力是協同合作業務。大型企業現在對潛在供應商之資料安全完整性進行廣泛的盡職調查，因為他們不想對關聯企業的資料洩漏承擔責任。

但是 GDPR 商業意識的提升也會產生負面影響：消費者會更加瞭解自己的資料權利。而且消費者會知道，如果一家公司無法控制他們的資料 (請注意：不一定要洩漏資料)，他們就有權獲得賠償。企業必須保持專注。



Sally Eaves
@sallyeaves

Sally Eaves Consultancy
執行長暨總監

「資料保護已成為企業能否贏得或失去信任的當務之急。」



第二部分 – 機構如何教導員工？



員工培訓：這幾個字 會讓員工大翻白眼

確保培訓內容引人入勝的更多原因。接受過培訓的員工比較不可能違反資料保護的理想實務。如果發生資料洩漏事件，只要您能證明您致力於為員工提供資料安全方面的培訓，資訊委員辦公室 (ICO) 的裁決將會更有利於您。



Rafael Bloom
@rafibloom73

Salvatore
總監

「我喜歡把資料視為一個供應鏈項目，資料的來源和整個生命週期都需要適當的管理。讓您的團隊待在一個房間內半小時並告訴他們該怎麼做、請不要撕碎東西、請設定理想的密碼。當然，您已經降低了組織的風險。但實際上，除了您對人員加諸的初始微幅影響以外，還有其他實質差異嗎？沒有。」

然而，在 2019 年 4 月，英國數位部長 Margot James 表示英國十分之三的組織已經為員工提供因應網路威脅的培訓¹。該是重視培訓的時候了。

這與培養文化有關，而不只是打勾訓練

培訓目的旨在影響真正的行為和文化變化，而不是打勾練習。購買線上培訓套件很簡單，這些套件會包含一些任何人都能正確回答的簡單資料保護問題。但這真的有助於保護您的組織嗎？

理想的資料保護行為有兩個基礎要素。首先，進行明智且具體的培訓，讓您的組織準備迎接獨特的挑戰。其次，意識到 GDPR 是一個強烈的職場文化問題，每天都會影響所有的員工。這是關於在整個組織中正確使用資料的正確方法。舉人力資源部門為例。想想所有應徵者的個人資料都放在電子郵件伺服器上。資料保護是每個人的責任。

1. Intelligent CISO：經過一年的時間，GDPR 對資料保護有何影響？
www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [存取時間：2019 年 11 月 26 日]



資料背後都代表一個人

在第一部分中，我們注意到消費者越來越清楚自己的資料權利。定位資料保護培訓的理想作法是協助員工進行交流，因為資料背後都代表一個人。讓您的員工想想他們曾經為其提供資料的每個組織，他們就會意識到資料保護攸關於個人隱私。

制定應變計劃



Sally Eaves
@sallyeaves

「持續對員工進行資料安全和隱私權方面的教育，是企業的當務之急。這絕對不是一次性、每年一次的培訓課程，而是一種主動、互動和引人入勝的體驗，因此是日常工作經驗的一部分。員工必須參與我們想要緩解、管理和抵禦風險的對話。」



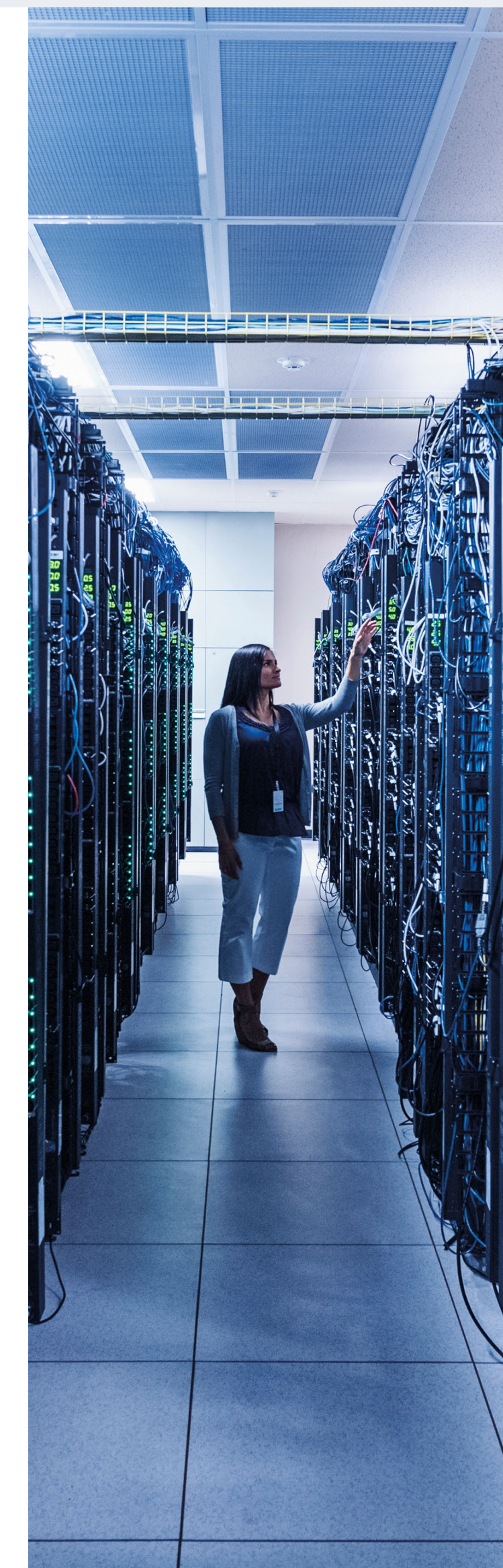
Miriam Brown
@Kingston_MBrown

「我認為在培訓期間，當您對別人說下列的話時，感覺很有趣：'如果這是您的資料該怎麼辦？如果我的銀行經理在家使用筆記型電腦工作，而這部筆記型電腦具有機密資訊，我會希望資訊位於加密的磁碟機中。」



Rob Allen
@Rob_A_kingston

「處理別人的資料時，要像處理自己的資料一樣小心。」



第三部分 - IT 部門能夠更妥善地保護裝置嗎？

遠端工作已經成為新常態

您的員工可能透過數種不同的裝置存取工作內容，包含很容易遺留在火車上或丟在計程車上的個人裝置。您面臨的挑戰是找出一個方法，讓員工能有效率地工作，同時不會面臨安全風險和資料洩漏的威脅。只要一個人，就能讓您的資料保護工作功虧一簣。

雙因素認證

對一般組織而言，截至目前，您所能做最理想且最簡單的事情就是保護網路安全邊界，而且那就像使用密碼管理程式和雙因素認證一樣簡單。雙因素認證的理想範例是，系統會提示使用者在筆記型電腦上輸入密碼，並在成功輸入密碼後發送到手機。

VPN 和加密的 SSD/USB

VPN 在中小企業 (SME) 越來越受歡迎。這對於透過公共 WIFI 網路取得業務資料的員工而言特別重要。但企業必須小心，不能高估 VPN 的能力。他們屬於解決方案的一部分，但不代表整個解決方案。企業經常部署 VPN，但目的只是為了讓遠端工作者使用筆記型電腦或膝上型電腦，而不需進行硬體加密。幾乎每個人都把檔案儲存在膝上型電腦上。如果該裝置遭到駭客入侵、遺失或遭竊，該怎麼辦？加密 USB 和 SSD 的價格只比標準版本略貴一些。部署加密的 USB 以及為筆記型電腦配備加密 SSD 固態硬碟，可為遠端工作者解決許多挑戰。如果裝置遺失或遭竊，您大可放心，因為沒有人可以存取加密的檔案。您甚至可以遠端銷毀遺失的 USB。



Sally Eaves
@sallyeaves

Sally Eaves Consultancy
執行長暨總監

「在傳輸、靜止和使用時，資料都需要受到保護 - 重要的是制定全方位的安全性、復原及資料清除計劃，以涵蓋上述的所有內容。關注經常被低估的風險領域極為重要，例如，未加密的 USB、使用電子郵件發送未加密的附件，以及會暴露敏感性使用者資料的網路瀏覽器功能。隨著許多互連裝置和工作模式不斷演進，請務必確保儲存在手機中的資料與儲存在公司伺服器的資料安全無虞。」



「我曾經遇到一位網路安全專家，他試圖說服一家公司的執行長採用雙因素認證，卻遭到拒絕：『不，我們不想這樣做，這樣很麻煩，這是個多餘的步驟，我不想這樣。不久後，他們變成一起 4 萬英鎊詐欺案的受害者。』」

Rafael Bloom
@rafibloom73

Salvatore Ltd
總監



「最終，提高安全意識的最佳方式是與員工進行對話，找到既安全又有效的策略。」

Rob Allen
@Rob_A_kingston

Kingston Technology
行銷與技術服務總監

專用伺服器 and MSP

有越來越多的大型組織正朝再次擁有現場伺服器的目標邁進。這代表他們能完全控制專屬的伺服器，而不會將任何資料儲存在可供公眾存取的雲端。還有一種混合伺服器解決方案，其中非敏感資料會保留在雲端，而個人資料則會保留在現場。對於第三部門的中小企業 (SME) 和組織而言，擁有專屬的伺服器成本可能太高。這就是託管服務提供者和虛擬專用伺服器的用處。這可提升對安全性的關注，而不會大幅增加營運成本

自動標記過期資料

GDPR 的宗旨之一是需要刪除舊資料。例如，某些類型之個人資料的保存時間不得超過 7 年。如果資料即將「到期」，系統會自動通知您嗎？有了正確的資料庫，當您的資料接近保留截止日時，您的 IT 團隊就可以輕鬆建立一個動作並向 DPO 發送自動產生的電子郵件。

與適當的廠商合作

談到 IT 安全性，有無數的製造商和廠商可供選擇。請好好研究。重要的擁有具有特定專業知識之受信任提供者所制定的系統，而可讓您所屬產業或部門的組織發揮能力。確保您選擇的廠商不僅擁有技術，並且瞭解資料安全性方面的採用挑戰。



第四部份 – 技術提供者如何改善流程和加強理解？



DPO 的 TLC

自 2016 年以來，對資料保護專員的需求激增 700%¹ 以上。目前全歐洲僱用的 DPO 超過 50 萬名，這是 2017 年²時預測數量的六倍。然而，DPO 角色的重要性卻常常遭到忽略和貶低。

DPO 要求全面了解您公司的安全性和資料隱私權狀況。這是一份全職的工作。然而在某些組織中，「DPO」卻只是指派給最瞭解技術的之職員的職務。他們要對整個公司的資料隱私權負責，同時還要履行日常工作職責。

事實上，需要廣泛的專業服務和工具，才能支援新型 DPO 的需求。即使您擁有全職的 DPO，由於資料安全性演進迅速，總會面臨需要有人提供第二觀點的挑戰。在資料安全性方面，與外部諮詢人員或顧問合作仍是漫漫長路，但您必須先在公司內把事情安排的井井有條。

清晰度、偶然事件和凝聚力

IT 基礎架構的強大能力取決於其最脆弱的部分。對於 IT 生態系統中的任何新成員，您的技術提供者應該就潛在的安全威脅提供清晰的資訊，並針對如何安全使用新產品提供明確的建議。



Tara Taubman-Bassirian
@clarinette02

GDPR、資料保護
和 IP 顧問

「我試著向各地安裝閉路電視攝影機 (CCTV) 的人們解釋，這並非絕對安全，因為安裝攝影機時通常不會設定密碼。因此，您可以直接登入網站，坐下來觀看。實際上這是在告訴強盜：「我不在的時候，你可以過來看看！」

1. Varonis：實施 GDPR 的一年：統計數據與要點須知
www.varonis.com/blog/gdpr-effect-review/ [存取時間：2019 年 11 月 26 日]
2. 《衛報》：GDPR 罰款：英航和萬豪的三億英鎊將何去何從？
www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [存取時間：2019 年 11 月 26 日]

還有一個偶然事件問題。當產品達到使用壽命或需要更新時，會發生什麼事？技術提供者應在產品上提供應急建議，以免無意中破壞其持有的資料，或是在較廣泛的 IT 生態系統中暴露安全性風險。舉 MRI 掃描為例。它可能具有 4 TB 的加密 SSD 固態硬碟，以儲存患者的影像。但如果儲存空間不夠時，會發生什麼事？

技術提供者和組織也必須推動數位凝聚和資料凝聚的環境，同時在內部組織內，以及與外部供應商和合作夥伴一起工作時。對於 NHS 此類多面向、多部門和多據點的組織而言，這點至為關鍵。

地平線掃描

科技快速發展，有時甚至會超越安全性。隨著新興科技的發展（例如中國的臉部識別支付技術），有時一些組織會競相使用該技術，而未先行考慮潛在的安全和資料保護後果。5G 網路的廣泛利用距離現在只有一兩年的時間，到時候邊緣運算 (Edge computing) 和分布資料孤島將成為現實。技術提供者必須能夠協助組織安全地從新興技術中受益，而不會損害其自身的資料完整性或 IT 安全性。



Miriam Brown
@Kingston_MBrown

Kingston Technology
B2B 策略行銷經理

「我們已經向 NHS 售出許多產品，但當我們詢問他們現有的資料保護政策和協定時，從一個信任到另一個信任之間有著明顯的差別。」



Sally Eaves
@sallyeaves

Sally Eaves Consultancy
執行長暨總監

「我相信我們將開始看到 GDPR 的變化，從減少實施的煩惱到專注於取得收益，例如增加 IT 流程、備份和復原，以及提高安全性，以及將這些作為在業界同儕之間脫穎而出的重要關鍵。」

GDPR 確實改變了企業，讓高層主管和消費者對資料隱私權和網路安全有所注意。然而，需要日復一日持續要求員工不斷地關注資料安全性，才能實現法規遵循性。技術和網路威脅不斷演進，這代表理想的安全基礎架構和理想培訓（以技術和資料隱私權的良好諮詢支援作為後盾），這對於所有企業至為關鍵。提醒員工在資料背後都代表一個人，這對於培養員工的資料保護文化很有幫助。而文化改變遠比逐項打勾培訓有用。





關於 Kingston

Kingston 擁有 32 年的豐富經驗，具備識別和解決遠端工作挑戰的知識，可輕鬆地讓您的員工在世界各地安全地工作，而不會對您的組織造成任何影響。

©2021 Kingston Technology Far East Corp. (Asia Headquarters), No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan.

版權所有，保留所有權利。所有商標 及註冊商標係屬於各自所有者之智慧財產權。

#KingstonIsWithYou