個資法來了，我該怎麼辦？

近年來國內重大個人資料外洩的事件屢見不鮮，如何保護客戶的個人隱私已經是全世界最重視的問題之一。客戶資料的外洩不但讓詐騙集團有機可乘，嚴重影響社會治安，更重創企業商譽，阻礙電子商務的應用及發展。所以在各界的關注和世界潮流的驅使之下，新版的個人資料保護法立法在即。

最新的個資法修正草案正在立法院如火如荼審查中，朝野兩黨也在已經對部份條文達成共識，主要修正要點包含了擴大保護客體、普遍適用主體、增修行為規範、強化行政監督等多項。其中對企業影響最深的莫過於以下三點(注 1)：

1. 擴大了適用範圍，**所有的公、民營事業均適用**。（刪除現行條文第 19 條至第 22 條）
2. 原先的**最大賠償金額**從新台幣兩千萬圓增至**新台幣五千萬圓**，如該原因事實所涉利益超過新臺幣五千萬元者，則以該所涉利益為限。（修正草案條文第 28 條第 4 項）
3. 非公務機關之代表人、管理人或其他有代表權人，**除能證明已盡防止義務者**，應並受同一罰鍰處罰，以加強其監督之責任。（修正草案條文第 46 條至第 49 條）

所以個人資料外洩的不再只是單一事件，巨大的賠償金額將會衝擊到企業的永續經營。當事件發生時還必須能夠證明已盡防止義務才能免責，處處都挑戰企業現有的資安防護措施與政策，面臨從所未見的嚴峻考驗。

身為企業資訊部門主管的您，該如何面對這次重大的考驗？其實我們只要能利用現有的工具，對內部資料、外寄(顯)資料、教育訓練等每一個環結個個突破，許多問題都會迎刃而解。

一、 內部資料的控管

大部份資訊外洩的根本原因都在於企業內部資訊管理成效不彰，文件並沒有適當的歸檔，也沒有確實分類和權限設定，因此才會讓公司內部有心人士透過各種漏洞來收集資訊。可惜的是就算我們知道有這些問題存在，還是難以有效的管理。其中最主要的因素就是**資料量太大**，**資料分散**在各伺服器或資料庫當中，想要稽核也無從查起。如果真得要狠下心來一一整理和確認檔案內容，恐怕要花費難以想像的人力和時間，在時效性上是完全不可行的。

我們必須提早發現公司問題，才能有效預防資訊外洩。一個功能完善的企業

搜尋引擎就可以解決您的難題。Openfind Enterprise Search(OES) 是一個整合企業內外部各種不同異質資料的搜尋平台，管理者只要透過簡單的關鍵字搜尋就能知道敏感性的資料存放在哪裡。進一步的去確認資料是否放在公司規定的地方、有沒有足夠權限設定。粗心的員工可能不小心將客戶個人資料放在權限過低的資料夾中，就可以即早發現並改正。

具有特殊性質的資料如，**電話號碼、信用卡號、身份證字號等**，可透過 OES 獨有的**特徵值比對技術**來搜尋，任何隱含個人資料的文件，就算是藏在 Word 檔中的小段落都將無所遁形，立刻被找出來。有些語意相關的關鍵字則可透過搜尋引擎的模糊搜尋和容錯能力來找到資料，例如您輸入『保險費』,『保費』的關鍵字內容也會找到。

內部資訊管理的重點在於要能夠在短時間內快速找到公司內部敏感資料存放的位置，我們就能夠重新評估資料的存放原則和存取權限設定，並在第一時間內防堵內部人員外洩個人資料的風險。而這一點就有賴於同時具有即時搜尋引擎核心、異質資料整合、特徵值搜尋、 Windows 檔案權限整合、巨量搜尋等技術的搜尋引擎 OES 來幫我們完成。

▲ 企業級搜尋引擎可輕鬆解決各類資訊系統資料量龐大及效率低落問題

二、 外寄(顯)資料的稽核

做好內部資料的控管是最基本的功夫，然而針對公佈在外的網站資料，或是透過 E-Mail 傳送出去的信件是否洩密，則是資安人員每日要戰戰兢兢應付的重要課題。

網站的稽核

網站已經是企業必要的行銷入口，許多重要的資訊或是與客戶的互動都是透過網站來運行。網站主要面對的難題有二：

1. 客戶上傳的分享資訊難以控管，Google 就有主管因不能即時對侵犯隱私的資訊下線而被判刑的例子(注 2)。
2. 許多網頁是連結到內部資料庫或是透過上稿軟體上傳的，難保程式沒有漏洞或是人為的失誤，導致隱私資料公開傳佈。。

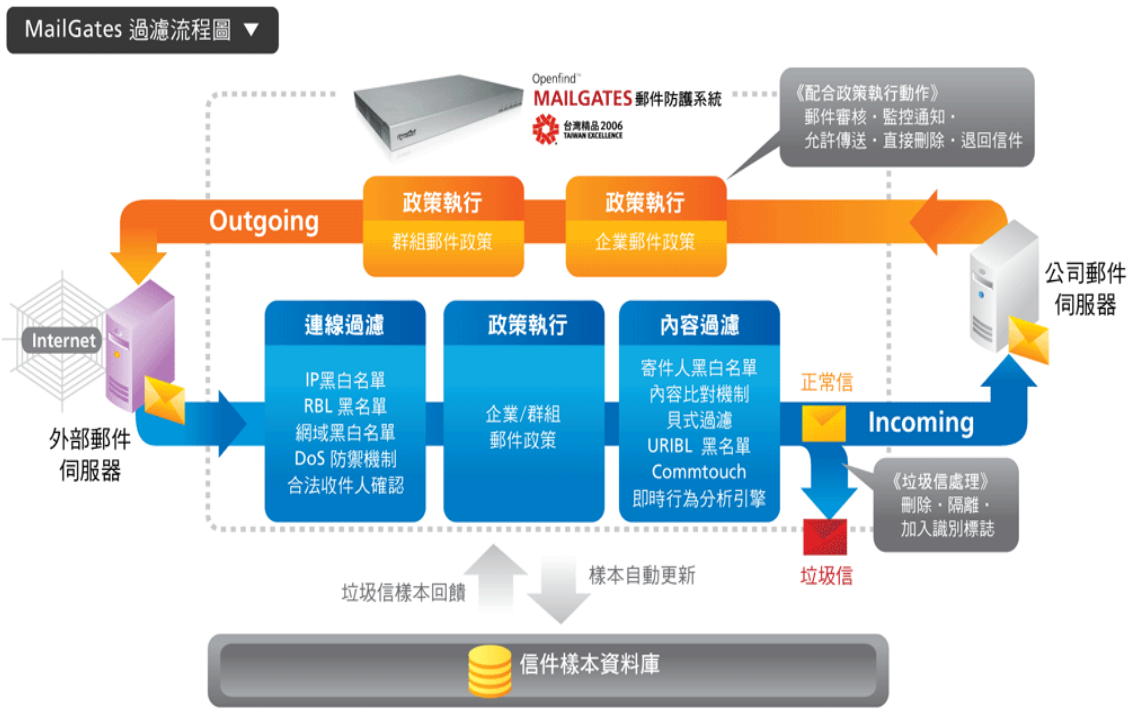
OES 在網站內容的稽核上扮演重要的角色，網站也是 OES 支援的資料來源之一，所以我們一樣可以透過關鍵字、特徵值等搜尋來對網站進行健檢，在短時間內找出有問題的網頁，快速把資料下線來降低傷害。

郵件的稽核

E-Mail 是現今最常用的溝通工具，所以也承擔著資訊外洩最大的風險。根據 Gartner 調查顯示，每 400 封信件當中，就有一封就隱含著機密資訊。針對 E-Mail 的處理措施，我們要從兩個觀點來探討：

1. 郵件即時稽核

針對公司外寄的所有信件，要能夠主動偵測是否內含不當的個人資訊，如果有，就要經過特別的審核與檢驗。我們可以用 MailGates(MG) 對外寄的郵件做即時稽核。MG 為一雙核心郵件防護系統，不但能抵擋垃圾信件、病毒信件、惡意程式與釣魚信件等攻擊，也可以對外寄的郵件設定多欄位的檢測規則。
檢測的範圍除了信件的欄位，附檔的內文也能做全文偵測，就算惡意的更改副檔名或是壓縮的檔案也可以被 MG 辨視出來。



2. 郵件備份與調閱

備份信件算是一件相對容易的事情，但是能夠在時間內**調閱大量的信件**，並且準確的找出含敏感資訊的信件才是管理者最應該要在意的事情。因為我們必須透過事後的稽核與調閱做為資訊外洩的補救措施或證明公司清白之依據。

MailBase(MB) 就是一個利用搜尋引擎協助快速調閱並且符合證據鏈保存(evidence chain of custody)要求之 Mail Archiving System。MB 本身內建搜尋引擎核心，可以快速的利用關鍵字搜尋大量的信件。在管理方面，所有使用人員的操作都會紀錄下來，沒有竄改信件的管道，以符合證據鏈保存要求。

完整和即時的歸檔　　完善的管理機制　　快速和安全的查詢

三、 人員教育訓練

許多工具可以幫您有效率的審查企業內外部各種資訊的內容，在第一時間內做好防範的措施。但最後還是要提醒您，正確的資安政策和員工的教育訓練才是預防資料外洩的根本。我們要時時刻刻教育和提高公司同仁的警覺性，把客戶的資料當成最重要的資產來處理。

個資法的通過是勢在必行，千萬不要等到通過之後再來臨時抱佛腳。即早審視企業內外部的資訊管理防護，預先對各種可能的個資外洩情況做演練，善用各種工具來稽核，個資外洩的問題就不再是惱人的問題。

1.台灣個人資料保護協會

http://www.elite-it.com.tw/TWPDA/company00_1_2.asp

2. 2010 年 2 月 25 日，霸凌影帶撤太慢 Google 主管判刑，聯合報，

http://www.udn.com/2010/2/25/NEWS/WORLD/WOR3/5438450.shtml