# 即刻做好萬全準備，以因應資料主體之近用要求

歐盟一般資料保護規範〈General Data Protection Regulation，簡稱 GDPR〉即將上路，雖然罰鍰加重（最高可達 2 千萬歐元或年度全球總營業額的 4%）成了眾所關注的焦點，但很多人卻忽略了「資料主體之近用權請求」〈Data Subject Access Request，簡稱 DSAR〉可能會對適用 GDPR 的組織（以下簡稱組織）帶來的諸多影響。

沒錯，DSAR 並非歐盟公民享有的「新」權利。既然如此，組織為何需要特別注意？資料主體所提出的近用權請求會有哪些變化？未來組織可能收到類似下方這封來自歐盟公民的信件，要求查閱組織說明是如何取得他的個人資料。

**Could you respond to a Data Subject Access Request?**

Good evening all,

Thanks from your email from spam@organisation.com

Could you please provide the following as outlined below (which under European data protection laws I'm legally entitled to be provided with as a **data subject access request**):

- Where, how and from whom you obtained my contact details?
- Where and how consent to send marketing information to my contact details was obtained?
- Details of all usages of my data (on a purpose by purpose basis – ideally, you might also please demonstrate what consent you obtained from me for each of those purposes)?
- Any privacy notice employed at the point my data was collected?

閱讀完整信件

舉個簡單的例子，GDPR 上路後組織將不能對資料主體提出的近用權申請收取手續費，這對企業組織會造成哪些影響？以愛爾蘭為例，組織可處理資料主體要求，並有權收取 6.35 歐元的費用。雖然這項機制看上去並不構成遏制的作用，但只要在回覆申請人〈資料主體〉的信函中說明手續費規定，往往就能讓對方打消申請的念頭。因此放棄申請要求的比例之高，可能會讓您感到驚訝，其原因在於該項費用通常無法以最簡便的現金或簽帳卡 / 信用卡支付，因此資料主體勢必

得使用其他方式付款，例如支票。有時候，這種麻煩事就足以讓極重視隱私權的資料主體打退堂鼓。可想而知，除去收費的障礙後，近用權申請量勢必增加。

我們通盤檢視了類似的因素，歸納出幾個組織可立即著手準備的方向，以確保 2018 年 5 月 25 日 GDPR 正式實施後，當組織面對蜂擁而至的近用權申請案時，能夠游刃有餘地處理並回應。

## 瞭解您持有的資料，以及何謂個資

所謂的資料保護並未涵蓋您所持有的所有類型的資料。該規範所涉及的資料，主要是可透過其原始形式或搭配持有組織所能取得之其他資訊，便足以辨識個人身分的資料。由此可知，這類資訊包括但不限於以下項目：

- 姓名
- 地址
- 出生日期
- 身高...

除此之外，還有一類是屬於敏感性個人資料。若要使用此類資料，除了須更確實地向蒐集資料的當事人徵求同意，亦應落實更嚴格的資料保護機制。這類資料包括但不限於下列項目：

- 性別傾向
- 健康紀錄
- 宗教信仰
- 工會成員身分

為確保組織能有效且高效率地處理相關案例，請務必參閱以下步驟，以便做好萬全準備，迎向 DSAR 的時代：

1. 與組織相關部門召開會議，釐清業務程序中的資料流程，並建立資料登錄機制
2. 建立容易施行的資料辨識、篩選及編寫程序
3. 考慮採用軟體或自動化解決方案，輔助資料的辨識、篩選及編寫作業，以回應 DSAR 申請

若不清楚現行程序的效果如何，不妨召集組織內部相關人員來場沙盤推演，確定實務上的實施成效。

## 時間是關鍵

依照現行法令，組織可以有 40 天的作業時間來回應 DSAR 申請。換言之，從收到資料主體的申請開始，便開始進入倒數階段。然而，當 GDPR 正式上路後，作業時間將縮短到 僅有 30 天，因此，組織在蒐集、審查、編寫（有必要的話）資料，以及將資料回覆給當事人的時間相當緊湊，很難有充裕的轉圜空間。若您從未經手 DSAR 相關業務，最好能先實際模擬，除了確定現行程序是否成熟到位，也能瞭解組織在處理這類資料申請時需要多少作業時間 （同時可瞭解這類業務將對組織的日常營運帶來哪些潛在負擔）。

## 別吝於向申請人索取更多資訊

別忘了，若您未確實識別資料主體，即貿然處理 DSAR 申請，可能會招來個資監管機關的關切，惹上麻煩。記住，只有當您收到當事人提供的充分資訊，並確定對方身分後，才有義務著手處理 DSAR 申請。確定身分的方式，包括附照片的有效身分證件及地址證明。

## DSAR 不得影響他人的權利與自由

雖然法律規定組織必須回應 DSAR 申請，允許資料主體取得其個人資料，但處理這類申請時，仍要留意不可影響其他人的權利與自由（當然，若能事先取得受影響當事人的同意，即可免除這方面的顧慮）。大多數情況下，您可適度編寫申請人以外之其他當事人的相關資料，至於實務上如何落實，則需由組織自行斟酌與決定，例如：是否需要使用軟體協助程序進行？或是，能否聘請專人檢查擷取出來的文件，將有必要編寫的地方塗黑以遮蔽資料？

## 確實記錄

最後一項建議，是在搜尋資料的過程中同步記錄。若資料主體後續提出其他問題，當初留下的紀錄就能助您一臂之力。萬一當事人向個資監管機關投訴，組織也能擁有正當立場，明哲保身。只要落實記錄機制，組織的資料處理程序就不太有機會招惹外界非議。

---

上述建議或許能協助您著手做好準備，但就如何處理 DSAR 案例及實施有效的政策與程序而言，各組織的狀況不盡相同，實際作法仍需由組織依自身需求量身訂做，可與 BSI 訓練學苑討論合適您的 GDPR 學習課程：

GDPR 基礎課程 1 天 GDPR 進階課程 2 天 BS 10012 主導稽核員課程 5 天

GDPR 基礎課程 2018/4/30、9/7 新班開課，點此了解>