不列顛船東責任互保協會
傳閱通告

西元 2018 年 7 月 31 日

主旨: 會員通用指南：歐盟第 2016/679 號「通用資料保護規則」實施作業

簡介：

歐盟(EU)2016/679 通用資料保護規則（以下稱 GDPR 或「保護規則」）於西元 2018 年 5 月 25 日正式生效，直接影響地區為歐盟/歐洲經濟體成員國[1]。英國並制定「西元 2018 年資料保護法」，確保國內法與 GDPR 接軌。歐盟保護規則全文共計 88 頁，請參見以下連結：
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en。

不列顛船東責任互保協會特別製作本指南，並在網站上持續更新資訊，藉此說明 GDPR 對協會及其會員的來往關係之影響。

保護規則適用效應最為明顯的層面是協會的人身傷亡、疾病索償及其他需要大量應用個人資料的理賠申請案處理作業。非個資相關或與自然人無涉（例如：公司）的資訊則不適用該規則。

保護規則的立法目的為取代歐盟第 95/46/EU 號指令，針對歐盟/歐洲經濟體內涉及個資收集、儲存、處理、調閱、使用、移轉、刪除等相關程序建構更為周密的保護框架，使保護標準趨於一致。在 GDPR 的規範下，個資「控管人」和「處理人」的責任範圍獲得清楚定義，讓歐盟/歐洲經濟體成員國內所有自然人均能獲得同等的法律權利保障，並利用相關監察與執行架構落實規範。

保護規則的適用對象如下：歐盟/歐洲經濟體成員國內持有個資者，位於歐盟/歐洲經濟體成員國境外但於歐盟/歐洲經濟體成員國境內提供貨物和服務者，或境外辦理資料移轉但個資接收人位於歐盟/歐洲經濟體者。

不列顛船東責任互保協會設址及營運地點均位於歐盟/歐洲經濟體境內，故本會所經辦之個資均屬 GDPR 適用範圍。本會成員與第三方服務供應商若在歐盟與歐洲經濟

[1] 本文所稱「歐盟/歐洲經濟體」係指歐盟成員國與歐洲自由貿易聯盟 (EFTA)三成員國（冰島、列支敦斯登、挪威）。

體境內營運且供應貨物或服務者，均須遵守本保護規則規範。歐盟與歐洲經濟體境內所持有之個資，即便資料當事人位於境外，相關作業同樣適用 GDPR 規則。

相關名詞定義[2]：

- **「個人資料」**係指與「資料主體」相關之任何資訊。
- **「資料主體」**係指有關身份已識別或足資識別的自然人或個人。足資識別的自然人係指可以直接或間接透過諸如姓名、身分識別證號碼、位置資料、線上識別碼等識別符號，或經由其他一項或多項身體、生理、基因、心理、經濟、文化、社會等身份特徵加以識別之自然人。
- **「控管人」**係指單獨或與他人共同決定個人資料處理之目的與方式的自然人、法人、公務機關、局處或其他機構等。
- **「處理人」**係指代控管者執行個人資料處理作業的自然人、法人、公務機關、局處或其他機構等。
- **「處理作業」**係指對個人資料或個人資料檔案執行之自動化或非自動化操作，例如資料收集、紀錄、組織、彙整、儲存、改編或變更、檢索、查閱、使用、傳輸揭露、散佈或以其他方式使之得以調整或組合、限制、刪除或銷毀。

不列顛船東責任互保協會、協會成員、保險經紀人、外部服務供應商、理賠申請人之角色定義

就 GDPR 之規範目的而言，不列顛船東責任互保協會係屬資料控管人。協會將日常管理事務外包給 Tindall Riley (Britannia) Ltd.（以下稱「TRB」公司）處理，故 TRB 為共同控管人。因為 TRB 已建立符合 GDPR 的管理規範，所以協會得在 GDPR 的保護框架下持續運行，TRB 也能以資料控管人或共同控管人的身份執行行政業務。TRB 也有代表協會與個資監管機構交涉的權力。

再者，屬於 GDPR 適用範圍的協會成員、保險經紀人、外部服務供應商如協會駐地聯絡員、律師、海事檢驗人員、專家等，因大多會各自獨立制定相關個資處理的目的與方式，故為保護規則定義之資料控管人。若「資料處理人」辦理範圍也包括資料處理的目的與方式的制定作業，就該部分的處理作業而言，該名處理人應認定為具備資料控管人身分。[3]

「資料控管人」與「資料處理人」身份的認定，舉例如：在人身傷亡或疾病給付理賠案等牽涉到個資的相關作業上有其重要性。理賠案的相關申請人為「資料主體」，享有 GDPR 給予的權利保障。

[2] 參見 GDPR 第 4 條。
[3] 參見 GDPR 第 28 條。

GDPR 相關規定：

- 個人資料處理原則
- 資料主體之權利
- 資料控管人和處理人權責範圍
- 向資料保護監管機關通報義務
- 資料保護長任命作業
- 個資移轉至第三國作業

個人資料處理原則[4]：

個人資料處理原則概要介紹如下：

- 合法性[5]：個資處理作業只得在有法律依據的前提下進行，例如：已徵得資訊主體同意者、基於履行合約之目的作業者、依法律規定作業者、基於保護資訊主體之重大利益，或資料控管人之合法利益之必要為處理作業等情形。
- 公平性：個資處理作業相關人員應向資料主體充分說明處理作業及資料主體權利。
- 透明性：說明資訊需簡明扼要且易懂。
- 目的限制原則：個資收集與持有目的須為特定、明確且合法，不得從事該等目的之外的個資處理。
- 資料最少蒐集原則：資料收集處理範圍僅限適當、相關且為處理目的所必要者。
- 正確性：個資應保持正確並隨時更新。
- 儲存限制原則：可用於識別資料主體身份之個人資料須以一定形式保存，儲存期間不得超過達成處理目的所需時間。
- 安全性：須採取適當措施保護個人資料的安全性，避免資料遭未經授權或非法利用，或發生意外滅失毀損等情事。

個人資料

[4] 參見 GDPR 第二章。
[5] 參見 GDPR 第 6 條。

個人資料處理作業僅得於符合特定條件的情況下執行，例如：已徵得明確同意者、基於建構法律主張、行使權利或辯護案件等作為之必要者，或法院執行司法權之必要者[6]。本會建議協會成員及其相關列名被保險人、經紀人、代理人等在合約、聘僱契約、勞資協定、船票載運條款等約定文書內加入符合 GDPR 規範的語句，藉此獲得相關當事人的同意，允許資料使用人處理敏感個資。GDPR 對處理未成年人的個資有較嚴格的規範，故這部分的合約語句在處理涉及未成年人的理賠案時益顯重要。

敏感個資應適用較為嚴格之特定規範，這些敏感個資包括資料主體之種族、民族背景和政治立場、以及健康與醫療資訊。

資料主體之權利[7]

以下概略列出資料主體享有之權利，包括資訊請求權：

- 透明原則和告知權：個資使用人應採行適當措施向資料主體說明必要資訊，包括資料控管人的詳細資訊和相關個資處理之作業目的。[8]另同樣應告知資料主體任何會接觸到相關個資的第三方資訊。
- 調閱權：資料主體有權要求個資使用人告知其個資是否進入處理作業與作業目的，並得請求調閱其個資相關處理資料。[9]
- 改正權：資料主體擁有請求更正錯誤資訊的權利。[10]
- 被遺忘權：資料主體在符合特定條件的前提下有權請求將其個資完全刪除，且不得刻意延誤。[11]
- 限制處理權：資料主體有權在特定情形下請求資料控管人對資料處理作業加以限制，適用情形的例子為當資料主體挑戰個資正確性的時候。

資料控管人、共同控管人、資料處理人之權責範圍

資料控管人和共同控管人

資料控管人和共同控管人應採行適當措施確保個人資料處理作業符合 GDPR 規範[12]，並制定推行「資料保護政策」和其他特定原則，例如：

[6] 參見 GDPR 第二章第 7 條和第 9 條。
[7] 參見 GDPR 第三章。
[8] 參見 GDPR 第三章第 12 條、第 13 條、第 14 條。
[9] 參見 GDPR 第三章第 15 條。
[10] 參見 GDPR 第三章第 16 條。
[11] 參見 GDPR 第三章第 17 條。
[12] 參見 GDPR 第四章第 24 條。

- 資料必要原則：制定程序確保資料處理範圍僅限於達成處理目的所必需的個資[13]
- 處理人：制定確保處理人落實符合規範的程序

資料控管人和共同控管人負責展示其作業遵循保護規定。[14]

不列顛船東責任互保協會和 TRB 為共同控管人。協會成員與其被保人就其從船員、代理人及其他第三方等處接收到的個人資料部分為控管人。

資料處理人

處理人須向控管人保證其採行之技術與組織管理措施的適當性，使資料處理作業符合 GDPR 規範，以保障資料主體的權利。[15] 控管人和處理人兩方需另行簽定符合特定規範的合約。

下列事項係屬控管人和處理人的責任範圍：

- 資料處理作業紀錄：應製作資料處理作業紀錄並加以保存，在監管機構檢查時配合提出。[16]
- 資料處理作業安全性：應制定適當的安全措施。[17]

向資料保護監管機關通報義務

若有違反個人資料之事宜[18]，導致資料主體的權利和自由受損，資料控管人應通報監管機關。若處理人得知有違反 GDPR 規範的案件發生，亦同樣負有向監管機關通報之義務。[19]

資料保護長

在特定情況，尤其是在需要大量處理個資的情形下[20]，應任命一名「資料保護長」(DPO)。資料保護長的責任業務包括監控各面向以確保符合 GDPR 規範，製作報告並提供內部諮詢。不列顛船東責任互保協會和 TRB 任命 Dan Wilkinson 先生為這兩間機構的 DPO。

資料移轉至第三國作業

[13] 參見 GDPR 第四章第 25 條。
[14] 參見 GDPR 第 5 條。
[15] 參見 GDPR 第 28 條。
[16] 參見 GDPR 第四章第 30 條。
[17] 參見 GDPR 第四 第 32 條。
[18] 參見 GDPR 第 33 條。
[19] _____(國家名) 的監管機關為 _____ (立法機構名)。
[20] 參見 GDPR 第四章第 37 條、38 條、39 條。

GDPR 規範之實施，讓歐盟全境對個資保護標準的預期趨於一致。因此，就個資安全性層面而言，由於歐盟/歐洲經濟體境內公司均須遵循同樣的規範，在境內各公司之間傳輸資料為合法行為。

若資料傳輸對象位於歐洲經濟體境外之國家，其移轉作業可經下列三種方式辦理：

1. 資料傳輸對象建議從業經歐盟認定為能確保個人資料保護程度足夠的國家名單選擇，國家名單連結為：https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en# dataprotectionincountriesoutsidetheeu。目前該名單收錄安道爾、阿根廷、加拿大（商業組織）、法羅群島、根西島、以色列、曼島、澤西、紐西蘭、瑞士、烏拉圭、美國 （若接收方為隱私護盾架構(Privacy Shield framework)註冊成員）等認定為提供充分保障的國家。目前日本和南韓正就充分保障的議題與相關方面協商中。
2. 建議個人資料移轉方與接收方簽訂資料保護的協議，作為個資獲得充分保護的保障。可適當採用歐盟標準示範契約條款(EU Standard Model Clauses)，網址為：https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en 。
3. 最後，特定個資移轉至歐盟境外國家或領地之作業存在 GDPR 遵循義務減免（放寬特定目的之條款）的情形，這種情形在移轉作業符合下列條件時適用：
   a. 移轉作業已徵得資料主體的同意;
   b. 資料控管人和他方簽訂促進資料主體利益之合約，資料移轉作業為履行該合約之必要行為；
   c. 資料移轉作業具備重大公共利益；
   d. 資料移轉作業為建構法律主張、行使權利或辯護案件等作為之必須；與
   e. 資料主體因身體之故或無法律行為能力而無法表示同意，但資料移轉為保護資料主體或其他人員的重大利益之必要作業。

GDPR 保護規則對不列顛船東責任互保協會和協會成員有何影響？應如何應對？

不列顛船東責任互保協會為因應 GDPR 的實施，已採取以下行動：

- 「資料保護政策」更新完成並實施中
- 特定資料保護長 DPO 任命完成
- 內部文書作業程序更新完成，修正內容包括加入定期文書審查以確保不必要的個人資料均已刪除。
- 以資料主體為收件人之標準隱私通知書準備完成，內含資料主體在 GDPR 規範下享有的權利之詳細說明，會在法規要求的時間點寄送。[21]
- 存有個人資料和敏感個資的資訊科技和通訊系統的安全性和完整性已完成驗證。

[21] 參見 GDPR 第 12 條。

對會員的其他影響

在 GDPR 的規範下，符合下列條件會員可能須採取類似的因應措施：在歐盟與歐洲經濟體境內營運者，位於歐盟/歐洲經濟體成員國境外但於歐盟/歐洲經濟體成員國境內提供貨物和服務者，位於歐盟/歐洲經濟體境內但持有境外人員的個資者。不列顛船東責任互保協會建議受影響的會員針對下述層面研議：

- 更新或制定資料保護政策，並實施之
- 個資處理量龐大的組織應考慮任命一名特定資料保護長
- 建構例行作業流程，確保資料主體能接收到與個資處理和自身權利相關資訊
- 非必需的個人資料應確實刪除或銷毀，但具備新的合法基礎故可繼續儲存者例外
- 應加強與第三方（包括其他船東責任互保協會在內）進行涉及符合敏感個資定義（例：健康或醫療資訊）之相關通訊的安全性。
- 為確保個資只能在受允許的情況下（例：具備合法基礎或另外簽訂合約者）移轉到第三國，應設置更多的檢核關卡。

違反懲罰

違反 GDPR 者所適用之懲罰刑度比舊法時代來得重許多。罰金金額係依個案內的特定因素裁定。裁量因素包括但不限於違反性質與期間、是否有採取減輕資料主體損失的措施等。這裡特別要強調的是，違反特定 GDPR 條文的懲罰很重，最高可處兩千萬歐元的罰金，若當事人為公司，則罰其前一會計年度全球營收的 4%，敬請注意。

本傳閱通告不具法律意見功能。會員在修正慣例作業流程時應向律師或當地資料監管機關尋求法律諮詢，以確保所有作業符合 GDPR 規範。

相關疑問或意見請聯絡 Dan Wilkinson 先生(電子郵件：dwilkinson@triley.co.uk)。