不列顛船東責任互保協會
傳閱通告

西元 2018 年 7 月 31 日

理賠案處理作業落實「通用資料保護規則」（以下稱 GDPR 或「保護規則」）說明

本傳閱通告發送之目的為向協會成員、駐地聯絡員及其他人員提供 GDPR 相關指引，減少觸法風險。本文並說明本協會之個資處理作業即將施行的各項修正。

對不列顛船東責任互保協會而言，人員相關的保險理賠案（例：船員或乘客的疾病給付和人身傷害理賠）是個資安全保障目標裡最具挑戰性的層面。

資料最小化原則 (data minimisation) 和隱私保護設計 (privacy by design)

在 GDPR 規範下，不列顛船東責任互保協會應認定為個資控管人，有證明其作業符合 GDPR 規定的義務。是故，為貫徹 GDPR 規範架構的主要原則「資料最小化(data minimisation)」和「從設計著手保護隱私(privacy by design)」（以下稱「隱私保護設計」），本協會計畫推行以下措施：

- 對經慣例作業流通的個資量加以限制
- 加強利用現有科技，確保個資移轉作業的安全性
- 盡可能使個資匿名化

由於電子郵件寄送名單持續增長之故，若有人在郵件討論串的收件人名單裡插入不該存在的收件人，往往難以察覺。再者，現在電子郵件詐騙橫行，偽裝成業內人士發送訊息的情況屢見不鮮。詐騙犯的意圖多半是詐取金錢利益，但回應詐騙郵件的行為本身也會導致不列顛船東責任互保協會持有之個資外洩的後果。

處理疾病給付或人身傷害請領案的作業過程往往需要在很短的時限內與世界各地的協會成員、駐地聯絡員、供應商等人交換敏感個資。在這種情況，清楚理解並落實 GDPR 規範原則的重要性益發顯著。

由於協會成員、經紀人、外部服務供應商（例：駐地聯絡員、海事檢驗人員、學者專家）本身就是資料控管人，因此本協會就個資相關事務歸納出優良操作指南，並整理成以下十項要點供讀者參考：

1. **尊重** – 推己及人，對他人個資保持尊重的態度。

2. **盡可能減少電子郵件傳輸或紙筆紀錄的個人資料量** – 個資產生和流通量越小就越容易保護。敬請將個資寄送範圍限制在為處理理賠案之必需者。

3. **網路安全** – 請確認電腦系統的安全性無虞，在寄送內含護照資訊、醫療報告、雇傭契約等資料的附件檔案時應使用安全保護措施，例如：設定密碼並透過安全郵件伺服器寄送。本協會使用強制加密裝置或入口網站保護資料安全。

4. **匿名化** – 請以識別符號（例：船員、經紀人、檢驗人員）代替個人姓名和生日。也可考慮採用其他如船名、事件性質、啟航港等識別符號搭配案件參號作資料識別。這種模式可套用在電子郵件的主旨標題和內文，並在可行的前提下擴大應用到理賠案的所有相關證明文件。若作業上遇到別無選擇必須明示姓名的情形，我們建議同份文件內與該姓名相關的識別資訊應越少越好。本協會未來包括理賠案件說明在內的通訊文書也會套用這種模式。我們的目標是推行新操作模式之後，除了直接負責處理理賠案的作業人員以外，其他人無從辨識該案當事人的身份。

5. **重新撰寫** – 如果作業人員實在無法避免說出特定人士的身份，那應就在該次通訊內完成識別，之後再重新撰寫一封新的電子郵件，以免個人資料在信件來往的討論串裡重複出現。

6. **「全部回覆？」**-- 在使用「全部回覆」的功能之前，請先檢查收件人名單，確保名單內所有人員都具備閱讀該封郵件的相關權限。

7. **使用業務用電子郵件地址**：請勿使用非業務用的私人或其他不安全的電子郵件帳號。

8. **淨空並上鎖** – 離開辦公桌時，請將桌面淨空，電腦螢幕上鎖。紙本資料須以安全的方式棄置。

9. **了解 GDPR 規範** – 請費心研究 GDPR 規範在貴公司商務上應如何應用及違反規定時的相關罰則。

10. **傳播指南內容** – 請向貴組織的每位人員宣傳本指南內容。

上述安全保護措施可將不列顛船東責任互保協會和協會成員在處理個資時所面對的風險降至最低，故本會建議讀者採用以上措施，並推行其他適合貴組織的相關因應方案。

GDPR 對歐盟/ 歐洲經濟體 (EU/EEA) 境內與境外聘僱的海員之域外效力[1]

「GDPR 通用規範」為題的通訊中曾說明 GDPR 的適用對象為在歐盟 (EU)/歐洲經濟體 (EEA) 境內設有營業據點且作業內容包括處理住在 EU/EEA 境內的 EU/EEA 籍自然人個資之船舶所有人(owner)、租傭船人(charterer)和／或其經理人。例如，船舶所有人將管理部門設在希臘，並指定希臘籍的高階主管到旗下船舶任職，這些人員的個資即屬 GDPR 保護範圍。

GDPR 在特定條件下具備域外效力。資料來源為 EU/EEA 境內但移轉至 EU/EEA 境外的情形即為一類。符合下列條件之一的船員招募作業即是用 GDPR 保護標準：

- 船舶所有人/管理人位於 EU/EEA 境內但從 EU/EEA 境外招募船員。
- 船舶所有人/管理人位於 EU/EEA 境外但從 EU/EEA 境內招募船員。
- 船舶所有人/管理人位於 EU/EEA 境外也從 EU/EEA 境外招募船員，但該船航線經過 EU/EEA，可能產生資料從 EU/EEA 境內傳輸到 EU/EEA 境外的情形。

許多協會成員聘用當地人力仲介公司負責從菲律賓、印度、烏克蘭等其他 EU/EEA 境外地區招募船員。由於船員是由營業據點位於 EA/EEA 境內的船舶所有人/管理人所聘僱，即使船員本身沒有 EU/EEA 成員國籍，其個資處理作業仍應適用 GDPR 保護標準。

以此類推，EU/EEA 境外的船舶所有人/管理人從 EU/EEA 境內聘僱員工，由於該公司要處理 EU/EEA 國籍人士的個資，故這部分的作業應適用 GDPR 保護規則。

船舶所有人在隱私層面的責任義務

不列顛船東責任互保協會在船員疾病給付和人身傷害理賠請領案的角色往往是船舶所有人雇主責任險的保險人。在這種情形，船舶所有人/管理人須告知船員該公司的保險人和相關第三方會接收到船員的個人資料。

[1] 本文的「EU/EEA」係指歐洲經濟體 (EEA)，由歐盟成員國和歐洲自由貿易聯盟 (ETFA) 三個成員國 (冰島、列支敦斯登、挪威) 組成。

我們猜想本協會大多數會員所簽訂的船員雇傭契約和勞資團體協約 (CBAs)的內文可能多半缺乏個資保護條款/通知，或現行條款雖有約定但仍需進行更新修正。因此，本會敬請各位成員注意履行對船員的告知義務。

本協會建議會員除了原已製作建立的通用隱私通知以外(又稱「資料通知書」(information notice)或「公平處理通知書」(fair processing notice))，並應考慮把以下關於疾病給付和人身傷害理賠請領的條文加入上開通知書裡:

- **會處理什麼樣的個資？** – 個人和財務方面資訊，以及牽涉到海員的個人身份、健康狀況、疾病和人身傷害詳情等敏感個資。
- **處理個資之理由** – 協助醫療與保險理賠案
- **處理個資的法律基礎** – 保護當事人重大利益，履行雇傭契約義務，對各種權利主張進行因應或抗辯，遵守法律或法定義務，包括為當事人投保等。
- **個資移轉對象？**– 設於 EU/EEA 境內與境外且負責船員當事人的理賠、治療、旅行、遣返等相關事務的保險公司、保險經紀人、健康醫療機構和法人等。
- **個資保存期間？**– 保存期間依雇傭期間、追訴時效和其他相關因素決定。但大原則是盡量縮短個資持有時間。

以上建議仍有未盡之處，儘管全部照做也無法保證作業上就完全符合 GDPR 規定，但至少可以確保會員能向不列顛船東責任互保協會提供理賠案件相關資訊而不違反 GDPR 規定。

此外，應在當地尋求特定法律諮詢。

本協會於西元 2018 年 7 月 31 日發行的傳閱通告內有其他的因應措施建議，請參見該期「對會員的影響」章節。