不列颠船东责任互保协会
传阅通告

公元 2018 年 7 月 31 日

理赔案处理作业落实「通用资料保护规则」（以下称 GDPR 或「保护规则」）说明

本传阅通告发送之目的为向协会成员、驻地联络员及其他人员提供 GDPR 相关指引，减少触法风险。本文并说明本协会之个资处理作业即将施行的各项修正。

对不列颠船东责任互保协会而言，人员相关的保险理赔案（例：船员或乘客的疾病给付和人身伤害理赔）是个资安全保障目标里最具挑战性的层面。

资料最小化原则 (data minimisation) 和隐私保护设计 (privacy by design)

在 GDPR 规范下，不列颠船东责任互保协会应认定为个资控管人，有证明其作业符合 GDPR 规定的义务。是故，为贯彻 GDPR 规范架构的主要原则「资料最小化(data minimisation)」和「从设计着手保护隐私(privacy by design)」（以下称「隐私保护设计」），本协会计划推行以下措施：

- 对经惯例作业流通的个资量加以限制
- 加强利用现有科技，确保个资移转作业的安全性
- 尽可能使个资匿名化

由于电子邮件寄送名单持续增长之故，若有人在邮件讨论串的收件人名单里插入不该存在的收件人，往往难以察觉。再者，现在电子邮件诈骗横行，伪装成业内人士发送讯息的情况屡见不鲜。诈骗犯的意图多半是诈取金钱利益，但响应诈骗邮件的行为本身也会导致不列颠船东责任互保协会持有之个资外泄的后果。

处理疾病给付或人身伤害请领案的作业过程往往需要在很短的时限内与世界各地的协会成员、驻地联络员、供货商等人交换敏感个资。在这种情况，清楚理解并落实 GDPR 规范原则的重要性益发显著。

由于协会成员、经纪人、外部服务供货商（例：驻地联络员、海事检验人员、学者专家）本身就是资料控管人，因此本协会就个资相关事务归纳出优良操作指南，并整理成以下十项要点供读者参考：

1. **尊重** – 推己及人，对他人个资保持尊重的态度。

2. **尽可能减少电子邮件传输或纸笔纪录的个人资料量** – 个资产生和流通量越小就越容易保护。敬请将个资寄送范围限制在为处理理赔案之必需者。

3. **网络安全** – 请确认计算机系统的安全性无虞，在寄送内含护照信息、医疗报告、雇佣契约等资料的附件档案时应使用安全保护措施，例如：设定密码并透过安全邮件服务器寄送。本协会使用强制加密装置或入口网站保护资料安全。

4. **匿名化** – 请以识别符号（例：船员、经纪人、检验人员）代替个人姓名和生日。也可考虑采用其他如船名、事件性质、启航港等识别符号搭配案件参号作资料识别。这种模式可套用在电子邮件的主旨标题和内文，并在可行的前提下扩大应用到理赔案的所有相关证明文件。若作业上遇到别无选择必须明示姓名的情形，我们建议同份文件内与该姓名相关的识别信息应越少越好。本协会未来包括理赔案件说明在内的通讯文书也会套用这种模式。我们的目标是推行新操作模式之后，除了直接负责处理理赔案的作业人员以外，其他人无从辨识该案当事人的身份。

5. **重新撰写** – 如果作业人员实在无法避免说出特定人士的身份，那应就在该次通讯内完成识别，之后再重新撰写一封新的电子邮件，以免个人资料在信件来往的讨论串里重复出现。

6. **「全部回复？」**-- 在使用「全部回复」的功能之前，请先检查收件人名单，确保名单内所有人员都具备阅读该封邮件的相关权限。

7. **使用业务用电子邮件地址**：请勿使用非业务用的私人或其他不安全的电子邮件账号。

8. **净空并上锁** – 离开办公桌时，请将桌面净空，电脑萤幕上锁。纸本资料须以安全的方式弃置。

9. **了解 GDPR 规范** – 请费心研究 GDPR 规范在贵公司商务上应如何应用及违反规定时的相关罚则。

10. **传播指南内容** – 请向贵组织的每位人员宣传本指南内容。

上述安全保护措施可将不列颠船东责任互保协会和协会成员在处理个资时所面对的风险降至最低，故本会建议读者采用以上措施，并推行其他适合贵组织的相关因应方案。

GDPR 对欧盟/ 欧洲经济体 (EU/EEA) 境内与境外聘雇的海员之域外效力[1]

「GDPR 通用规范」为题的通讯中曾说明 GDPR 的适用对象为在欧盟 (EU)/欧洲经济体 (EEA) 境内设有营业据点且作业内容包括处理住在 EU/EEA 境内的 EU/EEA 籍自然人个资之船舶所有人(owner)、租佣船人(charterer)和／或其经理人。例如，船舶所有人将管理部门设在希腊，并指定希腊籍的高阶主管到旗下船舶任职，这些人员的个资即属 GDPR 保护范围。

GDPR 在特定条件下具备域外效力。资料源为 EU/EEA 境内但移转至 EU/EEA 境外的情形即为一类。符合下列条件之一的船员招募作业即是用 GDPR 保护标准：

- 船舶所有人/管理人位于 EU/EEA 境内但从 EU/EEA 境外招募船员。
- 船舶所有人/管理人位于 EU/EEA 境外但从 EU/EEA 境内招募船员。
- 船舶所有人/管理人位于 EU/EEA 境外也从 EU/EEA 境外招募船员，但该船航线经过 EU/EEA，可能产生资料从 EU/EEA 境内传输到 EU/EEA 境外的情形。

许多协会成员聘用当地人力中介公司负责从菲律宾、印度、乌克兰等其他 EU/EEA 境外地区招募船员。由于船员是由营业据点位于 EA/EEA 境内的船舶所有人/管理人所聘雇，即使船员本身没有 EU/EEA 成员国籍，其个资处理作业仍应适用 GDPR 保护标准。

以此类推，EU/EEA 境外的船舶所有人/管理人从 EU/EEA 境内聘雇员工，由于该公司要处理 EU/EEA 国籍人士的个资，故这部分的作业应适用 GDPR 保护规则。

船舶所有人在隐私层面的责任义务

不列颠船东责任互保协会在船员疾病给付和人身伤害理赔请领案的角色往往是船舶所有人雇主责任险的保险人。在这种情形，船舶所有人/管理人须告知船员该公司的保险人和相关第三方会接收到船员的个人资料。

[1] 本文的「EU/EEA」是指歐洲經濟體 (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。

我们猜想本协会大多数会员所签订的船员雇佣契约和劳资团体协约 (CBAs)的内文可能多半缺乏个资保护条款/通知，或现行条款虽有约定但仍需进行更新修正。因此，本会敬请各位成员注意履行对船员的告知义务。

本协会建议会员除了原已制作建立的通用隐私通知以外(又称「资料通知书」(information notice)或「公平处理通知书」(fair processing notice))，并应考虑把以下关于疾病给付和人身伤害理赔请领的条文加入上开通知书里:

- **会处理什么样的个资？** – 个人和财务方面信息，以及牵涉到海员的个人身份、健康状况、疾病和人身伤害详情等敏感个资。
- **处理个资之理由** – 协助医疗与保险理赔案
- **处理个资的法律基础** – 保护当事人重大利益，履行雇佣契约义务，对各种权利主张进行因应或抗辩，遵守法律或法定义务，包括为当事人投保等。
- **个资移转对象？** – 设于 EU/EEA 境内与境外且负责船员当事人的理赔、治疗、旅行、遣返等相关事务的保险公司、保险经纪人、健康医疗机构和法人等。
- **个资保存期间？** – 保存期间依雇佣期间、追诉时效和其他相关因素决定。但大原则是尽量缩短个资持有时间。

以上建议仍有未尽之处，尽管全部照做也无法保证作业上就完全符合 GDPR 规定，但至少可以确保会员能向不列颠船东责任互保协会提供理赔案件相关信息而不违反 GDPR 规定。

此外，应在当地寻求特定法律咨询。

本协会于公元 2018 年 7 月 31 日发行的传阅通告内有其他的因应措施建议，请参见该期「对会员的影响」章节。