BRITANNIA P&I
TRUSTED SINCE 1855

CIRCULAR

不列颠船东责任互保协会
传阅通告

公元 2018 年 7 月 31 日

主旨：会员通用指南：欧盟第 2016/679 号「通用资料保护规则」实施作业

简介：

欧盟(EU)2016/679 通用资料保护规则（以下称 GDPR 或「保护规则」）于公元 2018 年 5 月 25 日正式生效，直接影响地区为欧盟/欧洲经济体成员国[1]。英国并制定「公元 2018 年资料保护法」，确保国内法与 GDPR 接轨。欧盟保护规则全文共计 88 页，请参见以下连结：
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en。

不列颠船东责任互保协会特别制作本指南，并在网站上持续更新资讯，藉此说明 GDPR 对协会及其会员的往来关系之影响。

保护规则适用效应最为明显的层面是协会的人身伤亡、疾病索偿及其他需要大量应用个人资料的理赔申请案处理作业。非个资相关或与自然人无涉（例如：公司）的资讯则不适用该规则。

保护规则的立法目的为取代欧盟第 95/46/EU 号指令，针对欧盟/欧洲经济体内涉及个资收集、储存、处理、调阅、使用、移转、删除等相关程序建构更为周密的保护框架，使保护标准趋于一致。在 GDPR 的规范下，个资「控管人」和「处理人」的责任范围的清楚定义，让欧盟/欧洲经济体成员国内所有自然人均能获得同等的法律权利保障，并利用相关监察与执行架构落实规范。

保护规则的适用对象如下：欧盟/欧洲经济体成员国内持有个资者，位于欧盟/欧洲经济体成员国境外但于欧盟/欧洲经济体成员国境内提供货物和服务者，或境外办理资料移转但个资接收人位于欧盟/欧洲经济体者。

不列颠船东责任互保协会设址及营运地点均位于欧盟/欧洲经济体境内，故本会所经办的个资均属 GDPR 适用范围。本会成员与第三方服务供货商若在欧盟与欧洲经济

[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）。

体境内营运且供应货物或服务者，均须遵守本保护规则规范。欧盟与欧洲经济体境内所持有之个资，即便资料当事人位于境外，相关作业同样适用 GDPR 规则。

相关名词定义[2]：

- 「**个人资料**」是指与「资料主体」相关之任何资讯。
- 「**资料主体**」是指有关身份已识别或足资识别的自然人或个人。足资识别的自然人是指可以直接或间接透过诸如姓名、身分识别证号码、位置资料、在线标识符等识别符号，或经由其他一项或多项身体、生理、基因、心理、经济、文化、社会等身份特征加以识别之自然人。
- 「**控管人**」是指单独或与他人共同决定个人资料处理之目的与方式的自然人、法人、公务机关、局处或其他机构等。
- 「**处理人**」是指代控管者执行个人资料处理作业的自然人、法人、公务机关、局处或其他机构等。
- 「**处理作业**」是指对个人资料或个人资料档案执行之自动化或非自动化操作，例如资料收集、纪录、组织、汇整、储存、改编或变更、检索、查阅、使用、传输揭露、散布或以其他方式使之得以调整或组合、限制、删除或销毁。

不列颠船东责任互保协会、协会成员、保险经纪人、外部服务供货商、理赔申请人之角色定义

就 GDPR 之规范目的而言，不列颠船东责任互保协会是属资料控管人。协会将日常管理事务外包给 Tindall Riley (Britannia) Ltd.（以下称「TRB」公司）处理，故 TRB 为共同控管人。因为 TRB 已建立符合 GDPR 的管理规范，所以协会得在 GDPR 的保护框架下持续运行，TRB 也能以资料控管人或共同控管人的身份执行行政业务。TRB 也有代表协会与个资监管机构交涉的权力。

再者，属于 GDPR 适用范围的协会成员、保险经纪人、外部服务供货商如协会驻地联络员、律师、海事检验人员、专家等，因大多会各自独立制定相关个资处理的目的与方式，故为保护规则定义之资料控管人。若「资料处理人」办理范围也包括资料处理的目的与方式的制定作业，就该部分的处理作业而言，该名处理人应认定为具备资料控管人身分。[3]

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

「资料控管人」与「资料处理人」身份的认定，举例如:在人身伤亡或疾病索偿理赔案等牵涉到个资的相关作业上有其重要性。理赔案的相关申请人为「资料主体」，享有 GDPR 给予的权利保障。

GDPR 相关规定：

- 个人资料处理原则
- 资料主体之权利
- 资料控管人和处理人权责范围
- 向资料保护监管机关通报义务
- 资料保护管理员任命作业
- 个资移转至第三国作业

个人资料处理原则[4]：

个人资料处理原则概要介绍如下：

- 合法性[5]：个资处理作业只得在有法律依据的前提下进行，例如：已征得资讯主体同意者、基于履行合约之目的作业者、依法律规定作业者、基于保护资讯主体之重大利益，或资料控管人之合法利益之必要为处理作业等情形。
- 公平性：个资处理作业相关人员应向资料主体充分说明处理作业及资料主体权利。
- 透明性：说明资讯需简明扼要且易懂。
- 目的限制原则：个资收集与持有目的须为特定、明确且合法，不得从事该等目的之外的个资处理。
- 资料最少蒐集原则：资料收集处理范围仅限适当、相关且为处理目的所必要者。
- 正确性：个资应保持正确并随时更新。
- 储存限制原则：可用于识别资料主体身份之个人资料须以一定形式保存，储存期间不得超过达成处理目的所需时间。

[4] 参見 GDPR 第二章。
[5] 參見 GDPR 第 6 條。

- 安全性：须采取适当措施保护个人资料的安全性，避免资料遭未经授权或非法利用，或发生意外灭失毁损等事情。

个人资料

个人资料处理作业仅得于符合特定条件的情况下执行，例如：已征得明确同意者、基于建构法律主张、行使权利或辩护案件等作为之必要者，或法院执行司法权之必要者[6]。本会建议协会成员及其相关列名被保险人、经纪人、代理人等在合约、聘雇契约、劳资协议、船票载运条款等约定文书内加入符合 GDPR 规范的语句，藉此获得相关当事人的同意，允许资料使用人处理敏感个资。GDPR 对处理未成年人的个资有较严格的规范，故这部分的合约语句在处理涉及未成年人的理赔案时益显重要。

敏感个资应适用较为严格之特定规范，这些敏感个资包括资料主体之种族、民族背景和政治立场、以及健康与医疗资讯。

资料主体之权利[7]

以下概略列出资料主体享有之权利，包括资讯请求权：

- 透明原则和告知权：个资使用人应实行适当措施向资料主体说明必要资讯，包括资料控管人的详细资讯和相关个资处理之作业目的。[8]另同样应告知资料主体任何会接触到相关个资的第三方资讯。

- 调阅权：资料主体有权要求个资使用人告知其个资是否进入处理作业与作业目的，并得请求调阅其个资相关处理资料。[9]

- 改正权：资料主体拥有请求更正错误资讯的权利。[10]

- 被遗忘权：资料主体在符合特定条件的前提下有权请求将其个资完全删除，且不得刻意延误。[11]

- 限制处理权：资料主体有权在特定情形下请求资料控管人对资料处理作业加以限制，适用情形的例子为当资料主体挑战个资正确性的时候。

资料控管人、共同控管人、资料处理人之权责范围

[6] 参見 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。

资料控管人和共同控管人

资料控管人和共同控管人应实行适当措施确保个人资料处理作业符合 GDPR 规范[12]，并制定推行「资料保护政策」和其他特定原则，例如：

- 资料必要原则：制定程序确保资料处理范围仅限于达成处理目的所必需的个资[13]
- 处理人：制定确保处理人落实符合规范的程序

资料控管人和共同控管人负责展示其作业遵循保护规定。[14]

不列颠船东责任互保协会和 TRB 为共同控管人。协会成员与其被保人就其从船员、代理人及其他第三方等处接收到的个人资料部分为控管人。

资料处理人

处理人须向控管人保证其实行之技术与组织管理措施的适当性，使资料处理作业符合 GDPR 规范，以保障资料主体的权利。[15] 控管人和处理人两方需另行签定符合特定规范的合约。

下列事项系属控管人和处理人的责任范围：

- 资料处理作业纪录：应制作资料处理作业纪录并加以保存，在监管机构检查时配合提出。[16]
- 资料处理作业安全性：应制定适当的安全措施。[17]

向资料保护监管机关通报义务

若有违反个人资料之事宜[18]，导致资料主体的权利和自由受损，资料控管人应通报监管机关。若处理人得知有违反 GDPR 规范的案件发生，亦同样负有向监管机关通报之义务。[19]

---

[12] 參見 GDPR 第四章第 24 條。
[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)。

资料保护管理员

在特定情况，尤其是在需要大量处理个资的情形下[20]，应任命一名「特定资料保护管理员」(DPO)。资料保护管理员的责任业务包括监控各面向以确保符合 GDPR 规范，制作报告并提供内部咨询。不列颠船东责任互保协会和 TRB 任命 Dan Wilkinson 先生为这两间机构的 DPO。

资料移转至第三国作业

GDPR 规范之实施，让欧盟全境对个资保护标准的预期趋于一致。因此，就个资安全性层面而言，由于欧盟/欧洲经济体境内公司均须遵循同样的规范，在境内各公司之间传输资料为合法行为。

若资料传输对象位于欧洲经济体境外之国家，其移转作业可经下列三种方式办理：

1. 资料传输对象建议从业经欧盟认定为能确保个人资料保护程度足够的国家名单选择，国家名单连结为：https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu。目前该名单收录安道尔、阿根廷、加拿大（商业组织）、法罗群岛、根西岛、以色列、曼岛、泽西、纽西兰、瑞士、乌拉圭、美国 （若接收方为隐私护盾架构(Privacy Shield framework)注册成员）等认定为提供充分保障的国家。目前日本和南韩正就充分保障的议题与相关方面协商中。
2. 建议个人资料移转方与接收方签订资料保护的协议，作为个资获得充分保护的保障。可适当采用欧盟标准示范契约条款(EU Standard Model Clauses)，网址为：https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en 。
3. 最后，特定个资移转至欧盟境外国家或领地之作业存在 GDPR 遵循义务减免（放宽特定目的之条款）的情形，这种情形在移转作业符合下列条件时适用：
   a. 移转作业已征得资料主体的同意;
   b. 资料控管人和他方签订促进资料主体利益之合约，资料移转作业为履行该合约之必要行为；
   c. 资料移转作业具备重大公共利益；
   d. 资料移转作业为建构法律主张、行使权利或辩护案件等作为之必须；与
   e. 资料主体因身体之故或无法律行为能力而无法表示同意，但资料移转为保护资料主体或其他人员的重大利益之必要作业。

[20] 参見 GDPR 第四章第 37 條、38 條、39 條。

GDPR 保护规则对不列颠船东责任互保协会和协会成员有何影响？应如何应对？

不列颠船东责任互保协会为因应 GDPR 的实施，已采取以下行动：

- 「资料保护政策」更新完成并实施中
- 特定资料保护管理员 DPO 任命完成
- 内部文书作业程序更新完成，修正内容包括加入定期文书审查以确保不必要的个人资料均已删除。
- 以资料主体为收件人之标准隐私通知书准备完成，内含资料主体在 GDPR 规范下享有的权利之详细说明，会在法规要求的时间点寄送。[21]
- 存有个人资料和敏感个资的资讯科技和通讯系统的安全性和完整性已完成验证。

对会员的其他影响

在 GDPR 的规范下，符合下列条件会员可能须采取类似的因应措施：在欧盟与欧洲经济体境内营运者，位于欧盟/欧洲经济体成员国境外但于欧盟/欧洲经济体成员国境内提供货物和服务者，位于欧盟/欧洲经济体境内但持有境外人员的个资者。不列颠船东责任互保协会建议受影响的会员针对下述层面研议：

- 更新或制定资料保护政策，并实施之
- 个资处理量庞大的组织应考虑任命一名特定资料保护管理员
- 建构例行作业流程，确保资料主体能接收到与个资处理和自身权利相关资讯
- 非必需的个人资料应确实删除或销毁，但具备新的合法基础故可继续储存者例外
- 应加强与第三方（包括其他船东责任互保协会在内）进行涉及符合敏感个资定义（例：健康或医疗资讯）之相关通讯的安全性。
- 为确保个资只能在受允许的情况下（例：具备合法基础或另外签订合约者）移转到第三国，应设置更多的检核关卡。

[21] 参見 GDPR 第 12 條。

违反惩罚

违反 GDPR 者所适用之惩罚刑度比旧法时代来得重许多。罚金金额是依个案内的特定因素裁定。裁量因素包括但不限于违反性质与期间、是否有采取减轻资料主体损失的措施等。这里特别要强调的是，违反特定 GDPR 条文的惩罚很重，最高可处两千万欧元的罚金，若当事人为公司，则罚其前一会计年度全球营收的 4%，敬请注意。

本传阅通告不具法律意见功能。会员在修正惯例作业流程时应向律师或当地资料监管机关寻求法律咨询，以确保所有作业符合 GDPR 规范。

相关疑问或意见请联络 Dan Wilkinson 先生（电子邮件：dwilkinson@triley.co.uk ）。