MARSH

观察 | 2018年9月

因违反欧盟的《通用数据保护条例》所致罚款和处罚：保险承保因地点、保单条款和其他因素而异

经过两年过渡期，欧盟的《通用数据保护条例》（GDPR）于2018年5月25日正式生效实施。该条例具有广泛而深远的影响，给全球数据保护领域带来了一场革命。根据该条例规定，公司主体应当审查并改进其隐私和数据保护做法，否则将面临高额罚款、处罚和其他因信息泄露通知、抗辩和恢复而产生的成本。

对很多企业而言，罚款和处罚的保险承保问题属于核心问题

自欧盟的《通用数据保护条例》正式生效实施起已数月有余，摆在许多利益相关人面前的一个主要问题就是如何将合规、不合规成本与公司的保单有机的关联起来。尽管我们做过很多情景假设，但请记住，任何与该条例及保险承保有关的问题都必须从保险合同本身入手。

由于潜在数额巨大、各地法律规定存在差异、尚无法庭相关判例以及可能在董事会成员中间引发强烈反响，因违反欧盟的《通用数据保护条例》所导致的罚款和处罚已成为很多企业关注的头等大事。欧盟的《通用数据保护条例》采用双层结构，违反该条例导致的罚款最高可达2000万欧元或者相关企业在全球收入的4%，以两者之中较高者为准。其它违反情形，可能被处以最高1000万欧元或者相关企业上一财政年度全球总营业额2%的罚款，以两者之中较高者为准。

“因违反欧盟的《通用数据保护条例》所导致的罚款和处罚能否获得保险承保仍不十分明朗。”

被保险人有一个共同的疑问，那就是“我们的保单是否承保我们所受到的罚款或处罚？”答案因情况不同而有所差异，影响因素包括保单条款和适用管辖法律。

要回答保险承保问题，首先应当审查相关公司的保险计划并了解哪些保单可能提供承保。在识别出可能提供承保的保单之后，对各相关保险合同的条款和条件进行详细审查，审查内容包括保单是否明示承保因违反欧盟的《通用数据保护条例》所导致的行政罚款、被保险人的地点以及保单适用法律规定等所有影响保单承保的关键因素。

由于此类罚款成本能否获得赔偿在很大程度上取决于上述因素，我们认为因违反欧盟的《通用数据保护条例》所导致的罚款和处罚能否获得保险承保仍不十分明朗，随着所在地区和相关承保人的不同，不确定性程度有所差异。

企业在了解保险承保问题时千万不能想当然，请务必仔细查看保单并咨询相关承保人、保险顾问和法律顾问。

欧盟地区：与欧盟的《通用数据保护条例》相关的保险承保情况分析

在欧盟，数据保护责任保险并不是一个新的概念。许多保单通常都会承保被保险人因数据泄露而面临的责任。因此，当违反情况出现时，被保险人会选择哪些保单呢？一般来说，他们会选择一般责任险、专业责任险（包含或不包含网络风险扩展条款）、法律费用保险、董责险以及网络风险保险等。

由于一般责任险和专业责任险保单提供的保险保障存在局限性，因此，尚未安排网络风险保险的企业有必要与保险公司协商，通过额外支付一定的保费成本，对其标准保险保障实施优化。那些希望为数据泄露所致额外成本寻求保险保障的企业更应如此。

保险保障的范围和可获得性存在差异，但是可能涵盖罚款和处罚

欧洲大陆

上述各类保单项下的网络风险保险通常只承保数据泄露或事故发生之后的成本，但是在很多情况下，达信通过谈判努力，成功促使保险责任条件进一步放宽。任何保险审查都必须将下列问题纳入考虑范围，即，当贵公司遭遇数据泄露或网络攻击事件时，保单如何帮助贵公司降低财务损失。这也就是说，首先应审查保险责任成立条款，然后再考察除外责任和分项限额。

在欧洲大陆，大约从2010年起，网络风险保单开始承保因违反欧盟的《通用数据保护条例》所导致的大部分后果，包括罚款，但前提是该罚款在相关司法管辖地是可保的。这就需要确定是否有必要修改网络风险保单，从而使数据泄露或事故发生之后的成本被纳入承保范围之内。

英国

在英国，标准网络风险保单对于监管事件的承保存在差异。我们所看到的大部分网络风险保单都会对罚款提供一定程度的保险保障（如果罚款在该地区是可保的）。然而，承保协议的具体条件可能存在非常大的差异，因此我们建议像欧洲大陆一样，企业应对保险责任成立条款进行审查。

举例来说，一家领先保险公司提供的保险保障仅承保因个人身份信息或公司数据丢失所导致的罚款和调查，这意味着其它与欧盟的《通用数据保护条例》相关的风险，例如被赋予遗忘权的所谓违反情形，都不在承保范围之内。

在英国，除网络风险保险外，还有某些险种对数据泄露提供一定形式的保险保障，例如公众责任险、雇主责任险、专业责任险以及法律费用保险等。在这些险种中，保险公司所采用的标准条款趋向于仅承保因数据泄露相关损害或损失导致的第三方赔偿以及相关法律抗辩成本。通常来说，对于一家企业因数据泄露而发生的其它成本和费用，例如数据泄露支持、通知和公关成本，这些条款则不提供承保。

另外，当前公众责任和雇主责任保单项下的保险保障通常与英国《1998年数据保护法案》的违反情形挂钩，因此需要进行保单修改，以确保英国《2008年数据保护法案》和欧盟的《通用数据保护条例》的违反情形可以获得同等保险保障。值得注意的是，一般责任险和专业责任险保单通常不承保罚款和处罚。

通常来说，在欧盟的《通用数据保护条例》颁布之后，英国的保险公司愿意继续提供保险保障。同时达信也看到，保险公司在某些公众责任险和雇主责任险保单中提供相关的分项限额，并要求投保人提供更多关于个人身份信息处理和为迎接条例生效实施所采取措施的资料。尽管原有的保险保障被保留下来，其限额水平可能受到进一步的限制。但无论如何，企业所遭受的行政罚款都不太可能获得承保。

能否获得保险承保：不确定，视各国具体情况而定

欧洲大陆和英国

因违反欧盟的《通用数据保护条例》所导致的罚款和处罚是否可以获得保险承保，欧盟各个国家的情况并不一致。欧盟的《通用数据保护条例》对此问题也无定论。一个关键的考量因素就是，相关监管机构是否做过关于其罚款不可从第三方获得追偿的规定。在英国，金融行为监管局明令禁止保险公司承保由该局对其监管之下的公司所处的罚款。到目前为止，我们尚不知晓英国信息专员公署对于因违反欧盟的《通用数据保护条例》所致行政罚款能否获得保险承保所持的态度。

另外一个考量因素就是司法管辖地。由于欧盟的《通用数据保护条例》对保险承保问题未做规定，所以欧盟各成员国以及各监管机构之间难免存在分歧。在这些国家和监管机构中，有的明令禁止保险公司承保行政罚款，有的尚未发表任何意见，有的表示不确定，还有的则支持保险承保。

保单所适用的管辖法律也是考量因素之一。因违反欧盟的《通用数据保护条例》所致罚款属于民事性质，但是按照法律规定欧盟各成员国也可以对违反个人数据保护的情形进行处罚。如果这些处罚属于刑事性质或者涉及被保险人故意违法或重大过失行为，那么将很可能无法获得保险承保。

由于各国情况不同，因此我们不应对欧盟整体做一刀切式的判断。更重要的是，对于因违反欧盟的《通用数据保护条例》所导致的罚款和处罚是否可以获得保险承保这一问题，不应只由保险公司、企业或经纪人回答，各国判例法应首先做出澄清。

值得注意的是，某些网络风险保险公司表示，如果允许，他们将寻求做出赔偿；而且，他们已经采纳相关建议，为其在某些情形下的赔偿意愿提供支持，但他们并未详细说明这些具体是指哪些情形。

“由于各国情况不同，因此我们不应对欧盟整体做一刀切式的判断。”

结论

位于欧盟国家的企业有可能获得一份其中包含监管罚款和处罚（例如因违反欧盟的《通用数据保护条例》所导致的罚款）保险承保条款的保单。然而企业应当注意，尽管该保单包含保险承保条款，但并不保证一定会做出响应。

罚款和处罚的追偿可能面临障碍，不同情形之间可能存在差异。举例来说，某些因素需要监管机构进行考量，例如故意行为除外条款的潜在影响。

企业应与自己的保险顾问密切合作，审查保险合同条款，尽最大努力优化保险保障范围。在此过程中，企业还应当考察各成员国以及保单签发地的法律法规情况（必要时与您的法律顾问开展合作）。

美国和加拿大：与欧盟的《通用数据保护条例》相关的保险承保情况分析

保险保障范围：美国和加拿大市场的演变

在美国和加拿大保险市场，大多数现成的网络风险保单针对欧盟的《通用数据保护条例》提供一定形式的保险保障，在此类保单中，网络风险事件即是保险责任触发因素，也就是说，数据泄露应对成本，例如法务和通知成本将在承保范围之内。标准的网络风险保单也可能承保因欧盟成员国数据保护机构采取监管行动所导致的相关抗辩成本。

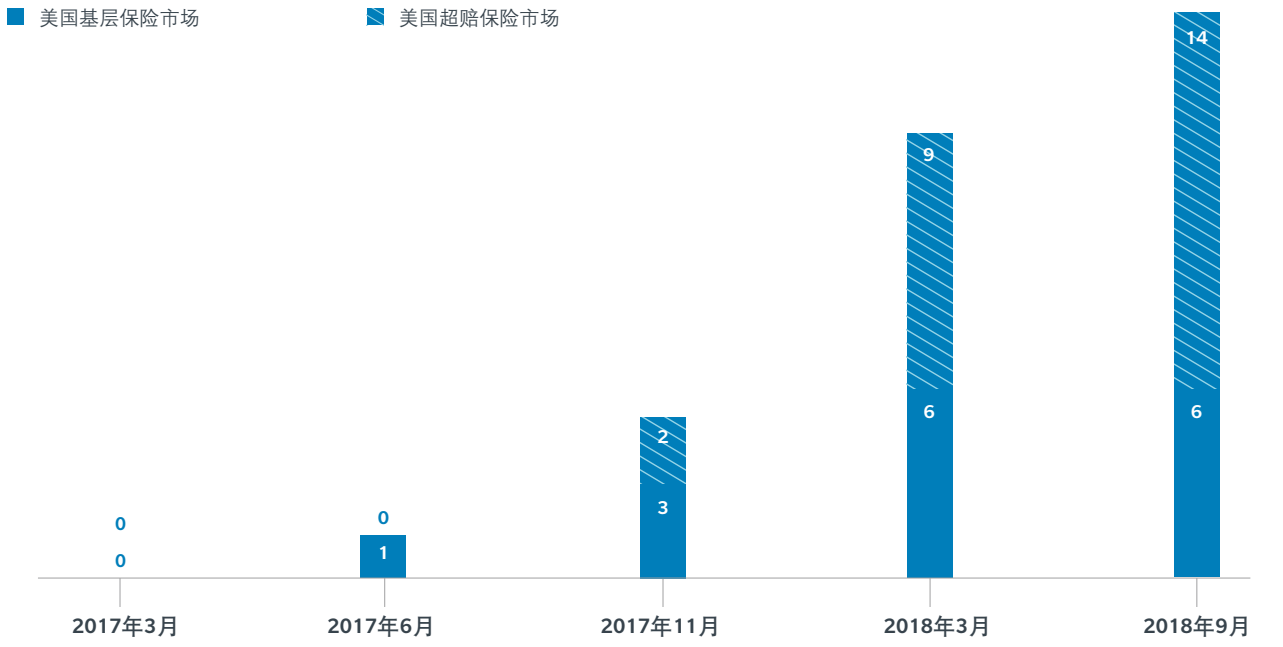
然而直到最近，在美国和加拿大签发的大多数网络风险保单仍不承保因企业隐私保护做法和合规问题所导致但保险责任并不一定由网络风险事件所触发的罚款和处罚。为识别这一潜在保险缺口，达信与美国和加拿大主要保险公司开展合作，在法律允许保险公司提供承保的地区，帮助多家客户获得了因违反欧盟的《通用数据保护条例》所致罚款和处罚的保险保障。

截至本文发稿时，至少有6家美国基层保险公司（在美国网络风险保险市场中，他们占有很大的市场份额）和5家加拿大大型基层保险公司或者同意修改保单条款以承保因违反欧盟的《通用数据保护条例》所导致的罚款和处罚，或者有意在现有条款中纳入对该类罚款和处罚的保险保障。

由于欧盟的《通用数据保护条例》所带来的监管风险非常复杂且不可预测，美国和加拿大的保险公司在保险承保方式和承保对象上存在很大差异。一些保险公司是否承保因违反欧盟的《通用数据保护条例》所致罚款和处罚需要视具体案例的情况而定，而另外一些保险公司则宽松很多。同样，一些保险公司要求相关被保险人回答更多核保问题或者提供其它补充信息。承保范围也有所差异，可能需要针对更多除外责任豁免或保单条款开展谈判，以便确保保单能够按照预期做出响应。

对于因违反欧盟的《通用数据保护条例》所导致的可保罚款和处罚，能够提供承保的美国和加拿大保险公司的数量

来源：达信分析



截至2018年9月，美国保险市场或者同意修改保单条款以承保因违反欧盟的《通用数据保护条例》所导致的罚款和处罚，或者有意在现有条款中纳入对该罚款和处罚的保险保障。

能否获得保险承保：地点可能对罚款和处罚的赔偿产生影响

美国

在欧盟成员国，因违反欧盟的《通用数据保护条例》所导致的罚款和处罚能否获得保险承保在很大程度上取决于成员国的法律和相关司法判决。然而在美国，地点可能会影响到罚款和处罚的赔偿。

截至2018年9月，达信已与多家主要保险公司达成协议，只要根据保险合同所适用的美国州法律推定被索赔罚款是可保的，他们将对美国公司做出赔偿。然而，其他保险公司也可能以公共政策规定（即欧盟成员国所开出的罚款显然是不可保的）为由拒绝赔偿。

尽管有上述情况存在，但是欧盟成员国法律关于罚款和处罚是否可保的规定并不是决定美国公司能否获得保险赔偿的唯一因素。目前有多家主要基层保险和超赔保险市场同意为美国地点提供承保，因此有效索赔无法获得赔偿的可能性不大。而且，在被保险人与其承保人开展理赔谈判的过程中，承保人可能会提供其它赔偿方案。

> *“达信已与多家主要保险公司达成协议，他们将赔偿美国公司因违反欧盟的《通用数据保护条例》所导致的可保罚款和处罚。”*

加拿大

在加拿大，罚款和处罚是否可保尚不明确。加拿大法院尚未直接处理过此类问题，但有评论指出，如果相关损失属于刑事性质，那么承保这些损失有违公共政策。当前一个悬而未决的问题就是民事或非刑事类罚款或处罚在加拿大是否可保。在加拿大法院做出相关判决之前，如果保险公司明示承保因违反欧盟的《通用数据保护条例》所致罚款和处罚，那么投保人可借此机会据理力争，争取获得保险赔偿。

结论

尽管从商业风险的角度看，因违反欧盟的《通用数据保护条例》所导致的罚款处罚能否获得保险承保存在不确定性，但是我们预计美国和加拿大的保险公司对于网络风险保险仍然秉持积极的态度。多家为美国公司提供承保的主要保险公司正在引入这一保险保障，而投保人无需为此多支付保费。因违反欧盟的《通用数据保护条例》所致罚款和处罚的保险承保问题也显示出美国和加拿大保险市场在过去和12-18个月中取得的巨大进步，越来越多的保险公司预计他们将针对该类罚款和处罚索赔提供保险赔偿。

达信针对欧盟的《通用数据保护条例》的评估服务和保险解决方案

达信在欧盟的《通用数据保护条例》生效实施之前已经做了多年准备工作，而且在许多市场获得了巨大的成功，通过在全球范围内设计保险条款，使客户面临的各项与欧盟的《通用数据保护条例》有关的成本都能够获得最佳的保险保障，包括法律规定可保的罚款和处罚。为满足客户的需求，我们为许多市场设计了专有的欧盟的《通用数据保护条例》保险条款，在我们看来，与保险公司提供的现成的保险条款相比，该保险单能够为条例相关风险和损失提供更加宽泛和高效的保险保障。

我们专有的评估服务和保险解决方案涵盖欧盟以及其它地区与欧盟的《通用数据保护条例》数据泄露相关的各种风险以及网络风险事件引发欧盟的《通用数据保护条例》问题时造成的财务后果。这些一流的工具和条款可与客户的总体网络风险管理计划实现无缝、高效融合，可提供潜在损失缓释解决方案，并对其它网络安全或风险转移产品形成补充，降低网络攻击发生的频率。

亚洲

在亚洲，有数家保险公司可以承保因违反欧盟的《通用数据保护条例》所导致的可保罚款和处罚。达信从法律顾问处得知，未来预计大多数亚洲主要市场都不会禁止保险公司承保该类保险。提供承保的保险公司也表示，如果法律允许，他们将对索赔做出赔付。当然，对于因违反欧盟的《通用数据保护条例》所导致的罚款和处罚在亚洲能否获得承保，被保险人应咨询法律顾问，获取相关法律建议。

澳大利亚

澳大利亚与英国类似，企业保单通常都提供隐私泄露保险，涵盖欧盟的《通用数据保护条例》的多个方面，包括澳大利亚法律允许承保的罚款和处罚。澳大利亚保险公司之间有一个共识，即在澳大利亚的企业因违反欧盟的《通用数据保护条例》所导致的罚款和处罚是可保的，但应注意的是，保单一般都会注明“在法律允许的情况下”。目前在澳大利亚，公开的保单考察活动是否会导致该项罚款或处罚无法获得承保，尚不明确。

百慕大

除此以外，还有其它保险市场可以承保因违反欧盟的《通用数据保护条例》所导致的罚款和处罚。例如，百慕大市场自很久以前就开始提供统括保险，承保在传统保险市场不可保的罚款/处罚。一家百慕大保险公司很快就会推出针对因违反欧盟的《通用数据保护条例》所致罚款和处罚的“分层统括保险”产品，另有几家保险公司正在敲定“分层统括保险”或条件差异“塔形统括保险”的保单条款。然而，由于首席基层承保人的不同，美国公司在某些情况下可能无法获得这些保险。

拉丁美洲

关于因违反欧盟的《通用数据保护条例》所致罚款和处罚是否可保的问题，拉丁美洲地区各监管机构一直保持沉默。然而，有数家保险公司向达信表示，只要不违反当地法律规定或监管要求，他们愿意提供承保。在墨西哥、巴拿马和秘鲁，虽然当地法律没有禁止保险公司承保因违反数据保护规定所导致的罚款或处罚，但是目前尚没有当地保险公司提供此类保险。

在巴西，虽然保险和再保险监管机构并未针对因违反欧盟的《通用数据保护条例》所致罚款和处罚是否可保这一问题做出明确规定，但是该国已经修改了法律规定，允许保险公司为监管机构收取的罚款提供保险承保。与其他地区的市场一样，该问题需由当地法院做出裁决。在阿根廷，因违反监管规定所导致的罚款和处罚无法获得保险承保。

在哥伦比亚，由监管机构采取的制裁措施，包括当地监管机构针对违反数据保护规定的制裁措施，是不可保的。在委内瑞拉，监管机构没有禁止此类保险，但是这属于新的保险产品，需要获得监管机构批准。

总之，在拉丁美洲地区，因违反欧盟的《通用数据保护条例》所导致的罚款和处罚是否可保，需要视当地保险公司的具体情况和监管机构的具体要求而定，这一点与全球其他保险市场是一致的。

结束语

欧盟的《通用数据保护条例》是对全球数据和隐私保护法规的重要补充，违规企业可能需要支付高额成本。高额的罚款和严苛的处罚已经引起许多企业的担忧，未来索赔是否可以获得保险保障的问题随之产生。达信认为，虽然答案取决于多种因素，例如保单条款和适用法律，但是在某些市场和某些情况下，保险保障仍然是可以获得的。

在这种环境下，尤其是在美国和加拿大市场（在全球网络风险保费中占比约90%），许多被保险人预计他们的保单将承保相关索赔，包括因违反欧盟的《通用数据保护条例》所导致的罚款和处罚。在达信组织的讨论中，许多美国和加拿大的大型保险公司表示他们预计将对索赔做出赔付。

财务及专业产品与欧盟的《通用数据保护条例》之间的关系是一个新的主题，尚未经过法庭澄清，还存在很多灰色地带和问题，有待法庭和保险市场进一步探索。重要的是，任何关于保险是否承保问题的讨论都应从保险合同着手，因为保险合同是保险范围和赔偿的基础。

保险是否承保受到多种因素影响，例如当地法律法规、监管结构以及保单条款等。

还有一点请谨记，罚款并不是企业面临的唯一财务风险。如果违反欧盟的《通用数据保护条例》、导致监管机构采取监管行动，那么企业还可能面临着法务取证、数据泄露通知、支持服务、对受影响数据主体的损害赔偿以及法律和/或监管抗辩等诸多方面的成本。因此，请务必检查您的保单限额，看其能否充分承保您面临的潜在财务风险 – 保险限额在罚款征收之前可能已经有所消耗。

最后，对于罚款和其它成本能否获得保险承保的问题，不要想当然。请与您的顾问携手合作，了解并（在可能和必要的情况下）尽最大努力扩展保单条款，从而使贵公司在面临欧盟的《通用数据保护条例》相关问题时能够最大程度获得保险赔付。

要点内容

欧盟的《通用数据保护条例》是一部影响深远的隐私和数据保护法规，随着它的正式生效实施，许多企业开始询问："我们的保单是否承保我们所受到的罚款或处罚？"

达信认为，在大多数市场，答案并非"是"或"否"那么简单 - 因违反欧盟的《通用数据保护条例》所导致的罚款和处罚能否获得保险承保取决于多个因素，包括：

保险合同约定

罚款或处罚的性质（刑事或民事），以及违反情形的严重程度。

法庭裁决（如果该问题进入法律流程）

被保险企业所在地点。在美国，地点可能关系到被保险人能否获得罚款和处罚赔偿。

亚洲
NAUREEN RASUL
网络风险部负责人
naureen.z.rasul@marsh.com
+852 2301 7206

百慕大
CARTER FRITH
高级副总裁
Bowring Marsh（百慕大） 有限公司
carter.frith@marsh.com
+1 441 299 8896

加拿大
CATHERINE EVANS
网络风险部负责人
catherine.evans@marsh.com
+1 416 868 7353

欧洲大陆
JEAN BAYON DE LA TOUR
网络发展部负责人
jean.bayondelatour@marsh.com
+33 1 41 34 50 05

拉美和加勒比
EDGAR TAUTA
业务持续性管理&网络风险部负责人
edgar.tauta@marsh.com
+57 3132894287

中东和北非
SIMON BELL
财务及专业责任险部负责人
simon.bell@marsh.com
+971 4 520 3846

太平洋地区
KELLY BUTLER
网络风险部负责人
Kelly.butler@marsh.com
+61 429 084 858

南非
JUSTIN KEEVY
部门主管
justin.keevy@marsh.com
+27 11 060 7377

英国
DAVID ARNOLD
高级副总裁
david.arnold@marsh.com
+44 (0)207 357 1759

美国
JEFFREY BATT
客户顾问，网络卓越运营中心
jeffrey.batt@marsh.com
+1 202 263 7880

THOMAS REAGAN
网络风险部负责人
thomas.reagan@marsh.com
+1 212 345 9452