聚焦数字经济监管：欧洲最强数据保护法处罚了哪些行为？

东方证券 ORIENT SECURITIES

研究结论

- 数字经济时代，如何更好地对互联网企业进行监管已经成为一个热点话题。针对这一内容，我们先后发布《聚焦数字经济监管：数字税会来吗？》、《聚焦数字经济监管：如何保护个人信息？》两篇报告。**本文我们将聚焦欧洲的数据监管，研究其法律框架建立之后哪些企业因哪些问题受到处罚，这些判例有助于我们形成对数据领域强监管的认识。虽然中欧之间国情差异较大，这种强监管的局面很难在国内形成，但考虑到《中华人民共和国个人信息保护法（草案）》已经出台，未来针对个人数据的保护有更加严格的趋势，从欧洲的经验中获得启发仍有意义。**
- 《通用数据保护条例》（General Data Protection Regulation，以下简称 GDPR）的特征包括：**（1）保护的关键对象是个人，企业等组织并不是 GDPR 的保护对象；**（2）明确了个人数据处理原则（包括合法公平透明原则、目的限制原则、数据最小化原则等七条）、数据主体权利（知情权、访问权、更正权、遗忘权等七项）等内容；（3）**含有判例法性质，判决结果一定程度上依赖于法官的主观判断，研究 GDPR 对企业运营的影响关键在于对判例的解读。**
- **监管重点影响的行业包括：（1）通信行业诉讼案例往往源于用户对激进促销活动的投诉，进而引起有关部门介入调查**，经典案例如 Wind Tre 通信公司在营销过程中，用户签署营销传播协议后无法撤回对此事的同意，隐私通知中提供的官方联系方式不可靠，提供的应用程序为了各种目的（如营销广告推送、地理定位）要求获得处理用户数据的许可，而这一许可需要等待 24 小时才能撤销，等等；（2）**互联网行业容易侵犯数据主体的知情权、有限处理权以及遗忘权，这限制了互联网企业通过大数据算法投放定制化广告的能力，除此之外，互联网行业还容易因为“长臂管辖原则”成为“数据共同控制者”承担次要责任。值得注意的是，部分跨国互联网巨头由于规模较大，很容易受到官方机构主动介入调查，**经典案例如剑桥分析公司利用 Facebook 数据帮助政治竞选团队定向投送政治类广告；（3）**由于金融监管制度的发展早于个人数据保护，相关法律法规已经趋于完善，所以并不是个人信息保护的侧重对象；**（4）对于航空、能源、物流、零售、房地产等非金融、非 IT、非互联网相关产业的企业来说来说， GDPR 更多关注数据主体知情权（有效同意）、遗忘权，个人数据处理原则中的数据最小化、限期储存原则，经典案例如法国家乐福会员注册数据保护条款信息冗长、不明晰且缺少关于数据保留的关键条例、非法使用 cookie 等等。
- 综上，数据监管框架的建立和完善对企业的影响主要有：（1）对客户信息的搜集分析对企业而言至关重要，但在数据监管框架下，需要什么样的数据（最小化原则）、用途是什么（目的限制原则）等等都受到全面监管，**定制化营销手段从而遭到挑战**；（2）第二，**供应链各个环节离不开员工等数据主体的个人数据，为达到监管要求，企业可能需要增加开支**；（3）传统的信息安全管理离不开员工技术能力和软硬件的支持，**企业需要增加培训以减少由于操作不当导致的数据泄露、建立规章制度以完善数据泄露的披露流程，这一因素将会利好一些提供网络安全相关服务的企业。**
- 风险提示：（1）跨国公司的数据监管涉及全球协调甚至在某些情况下关系到国家之间的博弈，具体政策落地与政策强度不确定性高；（2）监管相关机构执行力度与具体案例在社会上的伤害相比不高，从而监管执行效果不及预期。

报告发布日期 2021 年 02 月 21 日

证券分析师 陈至奕
021-63325888*6044
chenzhiyi@orientsec.com.cn
执业证书编号：S0860519090001

证券分析师 孙金霞
021-63325888*7590
sunjinxia@orientsec.com.cn
执业证书编号：S0860515070001

证券分析师 王仲尧
021-63325888*3267
wangzhongyao1@orientsec.com.cn
执业证书编号：S0860518050001

联系人 陈玮
chenwei3@orientsec.com.cn

相关报告

聚焦数字经济监管：平台经济反垄断指南正式发布	2021-02-17
聚焦数字经济监管：如何保护个人信息？	2021-01-05
聚焦数字经济监管：数字税会来吗？：——报告副标题	2021-01-03

专题报告

【宏观经济·证券研究报告】

数字经济时代，如何更好地监管互联网企业已经成为一个热点话题。针对这一内容，我们先后发布两篇报告，其中《聚焦数字经济监管：数字税会来吗？》探讨了数字经济时代国际税收制度安排的变化及其反垄断的功能，而《聚焦数字经济监管：如何保护个人信息？》则从数据隐私的角度，考察欧美在相应领域的做法，作为我国强化个人数据保护的借鉴。

本文我们将聚焦欧洲的数据监管，研究其法律框架建立之后哪些企业因哪些问题受到处罚，这些判例有助于我们形成对数据领域强监管的认识。虽然中欧之间国情差异较大，这种强监管的局面很难在国内形成，但考虑到《中华人民共和国个人信息保护法（草案）》已经出台，未来针对个人数据的保护有更加严格的趋势，从欧洲的经验中获得启发仍有意义。

GDPR 主要涉及权利与案例解析

如我们在《聚焦数字经济监管：如何保护个人信息？》中所介绍，欧盟于 2016 年颁布《通用数据保护条例》（General Data Protection Regulation，以下简称 GDPR），对个人在数据方面的权利作了深入、全面的规定，是欧洲数据治理体系的基础，也是全球范围内隐私保护的里程碑。

即使设置了两年过渡期，GDPR 依然在 2018 年打了众多公司一个措手不及。一方面，GDPR 各项原则含有普通法（判例法）的性质，判决结果一定程度上依赖于法官的主观判断，另一方面，条例中一些定义模糊之处（如数据主体、数据控制者、共同控制者等）还在更新迭代，各项权利的边界正在根据判例逐步细化与完善，研究 GDPR 对企业运营的影响关键在于对判例的解读。

主要涉及权利、原则及解释

GDPR 中关于数据主体“个人数据”定义指的是任何已识别或可识别的自然人（“数据主体”）相关的信息。一个可识别的自然人是一个能够被直接或间接识别的个体，特别是通过诸如姓名、身份编号、地址数据、网上标识或者自然人所特有的一项或多项的身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份而识别的个体。**GDPR 保护的关键对象是个人，企业等组织并不是 GDPR 的保护对象。**

涉及违反 GDPR 条例的案例主要涉及 GDPR 第 5 条个人数据处理原则、第 12-23 条数据主体的七项权利，以及第 32-34 条个人数据安全。在 Google、Facebook 等搜索引擎与社交平台的判例中还多次涉及有关数据控制者、共同控制者的判定。同一案例中数据控制者可能会由于有多项违规记录而加重惩处，也会因为数据控制者的规模、财力以及配合度酌情增减罚款金额。

GDPR 数据处理原则中确立了接收、处理个人数据的合法公平透明原则、目的限制原则、数据最小化原则、数据限期储存原则、准确性原则、完整性和保密性原则。这些原则对数据的控制者和处理者提出了严格要求。其中**目的限制原则、数据最小化原则、数据期限储存原则是案例中主要涉及的原则**，这三个原则在长度、广度与深度方面对企业处理敏感数据有严格的约束。敏感数据包含种族或民族背景、政治观念、宗教或哲学信仰、工会成员的个人数据、基因数据、为了识别特定自然人的生物性识别数据、以及和自然人健

康、个人性生活或性取向相关的数据。**GDPR 个人数据处理原则在大部分除数据泄露以外的案例都有体现，涉及行业包括但不限于电信供应商、能源公司、零售商、银行、物流、学术机构甚至是税收部门与公安机关。个人数据处理原则极大程度限制了平台个性化定制推送广告等依赖用户习惯大数据分析的潜在收入来源。**

个人数据安全案例主要涉及数据处理安全以及数据泄露报告机制。数据处理安全指的是控制者和处理者应当采取适当技术与组织方式，以保证和风险相匹配的安全水平，不同严重程度的数据泄露也与公司上报、配合的积极度有关。**个人数据安全案例平均罚款力度远高于其他案例，对企业维护网络安全与企业的信息安全防护能力提出了挑战。**

表 1：GDRP 个人数据处理原则、数据主体七项权利以及个人数据安全条例

个人数据处理原则（第 5 条）	数据主体七项权利（第 12-23 条）	个人数据安全（第 32-34 条）
合法、公平、透明原则	知情权	数据处理的安全性
目的限制原则	访问权	向监管机构报告对个人数据的泄露
数据最小化原则	更正权	向数据主体传达个人数据泄露
限期储存原则	遗忘权（擦除、删除权）	
准确性原则	限制处理权	
数据的完整性与保密性原则	数据携带权	
可问责性原则	反对权（含自动化）	

资料来源：GDPR，东方证券研究所

主要行业案例解析

案例一览

鉴于 GDPR 具有一定普通法（判例法）的性质，不同行业在同一原则下随着判例的增加会有不同的界限。目前 GDPR 判例在主要行业都已经有较为充足判例提供参考。

表 2：案件一览

时间	案件名称	违规背景简介	罚款金额（万欧元）
2018 年 5 月	意大利联合信贷银行数据泄露	技术问题导致客户数据泄露	13
2019 年 1 月	德国 N26 银行非法利用数据进行反洗钱	以“反洗钱”为由过久保存“前客户”数据	5
2019 年 8 月	保加利亚银行 DSK 数据泄露	技术问题导致客户私人信息泄露	51.1

2018 年 6 月	德国学术机构非法利用 Facebook cookie 采集用户数据	学术机构利用第三方软件非法采集，Facebook 没有做好数据安全保护	-
2020 年 5 月	芬兰物流公司	直接交易用户个人信息且未上报相关机构	10
2020 年 8 月	意大利 Wind Tre 非法处理客户数据	数据采集协议撤销困难并且将非法获得的数据用于营销等目的	1700
2020 年 1 月	意大利 TIM 非法处理客户数据	擅自利用客户私人数据进行个性化营销	2780
2019 年 12 月	意大利 EGL 非法处理客户数据	擅自利用客户私人数据进行个性化营销	1250
2021 年 1 月	德国零售商过度使用监控录像	对员工监控强度过高、录像保留期限太长	1040
-	法国家乐福数据保护条款冗长、非法处理数据、数据保留过长	数据采集同意协议不合规、违法采集 cookie 数据并用于数据处理	300
2019 年 7 月	英国万豪国际集团数据泄露	技术问题导致大量客户私人信息泄露以及披露不及时	11000
2020 年 7 月	丹麦酒店集团过度保留客户数据	过长保留顾客敏感信息	14.7675
2019 年 1 月	Google 非法使用安卓平台用户数据	数据过度分散、协议默认勾选同意导致数据采集协议无效	5000
2018 年 11 月	德国社交媒体公司客户登陆密码和电子邮件地址被窃取	由于技术问题导致客户数据泄露	20000
2018 年 9 月	AggregateIQ 公司&剑桥分析公司（Cambridge Analytica）政治广告违规案	非法采集、处理数据并用于政治广告投放	2000
2019 年 3 月	Facebook 未上报更换数据保护官	未及时上报数据保护官更换	5.1
2020 年 3 月	Google 没有合规行使数据遗忘权	未达到 2017 年监管部门的数据删除要求	700
2019 年 7 月	英国航空公司数据泄露	由于技术问题导致客户私人信息泄露	20000
2020 年 10 月	跨国快消品巨头 H&M 过度收集员工信息、非法监控员工隐私	由于技术问题导致员工私人信息泄露	3530
2019 年 11 月	法国巴黎银行罗马尼亚理财子没有及时回复客户删除需求	没有及时回复客户是否能够删除相关财务信息	0.2
	法国巴黎银行捷克理财子持有客户数据过久被罚	持有客户敏感信息过久	0.9704
2019 年 6 月	德国私人房地产因敏感数据存储过久被罚	持有租户敏感信息过久	1450

2018 年 9 月	奥地利博彩商店非法监控录像	监控拍摄范围超出商店	0.48
2020 年 4 月	荷兰某公司因为使用生物特征作为唯一考勤途径被罚	仅提供指纹作为唯一打卡考勤途径	72.5

资料来源：GDPR，www.enforcementtracker.com，www.nathantrust.com/gdpr-fines-penalties，东方证券研究所

备注：-代表数据缺失

通信、互联网相关行业

通信、互联网行业容易触犯数据主体的知情权、限制处理权，其次是遗忘权，监管关注的是数据处理过程是否满足合法公平透明原则、限制存储原则、数据最小化原则，这些要求极大限制了通信、互联网企业的销售能力，主要体现在限制了企业获取用户数据和利用用户数据进行定制化服务，从而弱化了盈利能力。除此之外，条例还对通信、互联网行业的安全技术与规范提出了较高的要求。

通信行业诉讼案例往往源于用户对激进促销活动的投诉，进而引起有关部门介入调查，用户满意度与被调查的可能性高度相关。有关部门重点关注三点：合同协议有效性、数据处理目的是否与协议不符、收集数据是否超出达成目的所必需。意大利最大的电信运营商 Tim 和第三大电信运营商 Wind Tre 分别在 2020 年 1 月和 2020 年 8 月收到意大利数据保护机构“Garante ”高达 2780 万欧元和 1700 万欧元的罚单。以 Wind Tre 为例，在收到大量关于 Wind Tre 激进促销的投诉后，Garante 对 Wind Tre 通信公司的营销活动进行了调查，发现这些通信并未得到用户的同意；还有一些用户抱怨签署营销传播协议后无法撤回对此事的同意，隐私通知中提供的官方联系方式也不可靠；另一项被 Garante 发现的违规行为是 Wind Tre 的应用程序“MyWind”和“My3”为了各种目的（如营销广告推送、地理定位）要求获得处理用户数据的许可，每次用户登录时都必须提供该许可，之后要等待 24 小时才能撤销。Garante 认为 Wind Tre 严重违反 GDPR 第 5 条、第 6 条关于数据处理合法性、第 17 条关于数据遗忘权，其侵犯具体体现在 Wind Tre 没有得到客户的有效同意（知情权），在同意的客户中也侵犯了有限处理权，违反了“数据最小化”原则，甚至拒绝客户行使数据遗忘权。

互联网行业与通信行业面临的合规风险类似，容易侵犯数据主体的知情权、限制处理权以及遗忘权，这限制了互联网企业通过大数据算法投放定制化广告的能力，除此之外，互联网行业还容易因为“长臂管辖原则”成为“数据共同控制者”承担次要责任，对平台数据保护提出了更高要求。值得注意的是，部分跨国互联网巨头由于规模较大，很容易受到官方机构主动介入调查。Google2019 年 1 月面临法国国家信息与通信委员会 CNIL 的调查，最终因违反透明原则，以及“未能为用于广告个性化目的数据提供法律依据”被 CNIL 罚款 5000 万欧元，具体原因在于，尽管 Google 已经获得了用户同意才进行数据处理并展开个性化的广告操作，但 CNIL 认为这一同意并不 “有效”：首先，用户个人信息被分散在 Youtube、Google 搜索、Google 主页、Google 地图、Playstore、Google 图片等等应用之中，无法被用户轻易、完整地访问；其次，用户的“同意”既不具体也不清晰，创建帐户后，用户被默认勾选显示个性化广告，但根据 GDPR 的规定，只有用户采取明确

的肯定动作（例如勾选未预先勾选的方框）的同意才是“明确的”。综上，CNIL 认为 Google 没有完全遵守 GDPR 中关于同意必须是“明确具体的”相关规定。

互联网公司关于执行数据主体遗忘权已有渊源，早在《95 指令》（欧盟于 1995 年颁布的《数据保护指令》，GDPR 的前身）下，著名的冈萨雷斯诉 Google 案已对此有明确的义务划分，当前互联网公司侵犯遗忘权的案例一般是由于遗忘权执行不规范导致的。冈萨雷斯诉 Google 案的经过为：2010 年，西班牙籍律师冈萨雷斯向西班牙数据保护监管局（AEPD）提交了一份针对西班牙先锋报、Google 西班牙分部以及 Google 公司的投诉，冈萨雷斯称当用户在 Google 上搜索自己姓名的时候，会搜索得到 1998 年《先锋报》两页新闻的链接，内容是为了清偿冈萨雷斯欠下的社会保险债务而要强制拍卖他的财产。冈萨雷斯认为这一强制拍卖措施多年以前就已经结束，这些信息也已经失效，于是请求西班牙数据保护监管局命令《先锋报》移除或者修改这些页面从而确保他的这些个人数据不能通过搜索引擎获取到，此外，他还请求西班牙数据保护监管局命令 Google 西班牙分部和 Google 公司删除有关他个人数据的这些链接。该案的最终结果为 Google 败诉，应删除搜索结果列表中的链接，这意味着，如果数据主体合理行使遗忘权，互联网平台仅有义务删除自己的数据库内容以及从搜索结果列表中删除由第三方发布的、包含个人信息且与该主体名字关联的网页，同时，根据《欧盟基本权利宪章》第 11 条第 1 款规定的言论自由权（GDPR 以欧盟法律、成员国法律为前提），互联网企业没有义务也没有必要通知相关报道的报社、媒体删除相关文章。

近年来有不少案例涉及遗忘权。仍以 Google 为例，2017 年，瑞典数据保护机关 DPA 对 Google 遗忘权的执行情况进行了一次审查，认为应删除若干搜索结果列表。2018 年，由于有迹象表明 Google 没有完全遵守这一指令，瑞典 DPA 发起了后续审核，发现当 Google 删除搜索结果列表时，会以某种方式告知链接指向的网站，从而使网站所有者了解到哪个网页链接被删、以及谁是请求遗忘权的主张者之后，可以将有问题的网页重新发布到另一个网址，新页面就会重新出现在 Google 搜索中，请求遗忘权近乎无效（删除搜索结果列表同时告知网站所有者的行为没有法律依据）。在此背景下，DPA 要求 Google 停止这一行为，并对 Google 处以 7500 万瑞典克朗（约 700 万欧元）罚款。

除此之外互联网企业还容易因为数据安全问题而承担连带责任。Facebook 在著名的剑桥分析公司丑闻中就承担了“共同控制者”的角色。这一案件较为复杂，控制者总共违反了第 5 条、第 6 条关于数据处理合法性、第 20 条有关数据可携权（数据迁移）、第 32.1 条确保个人数据安全的义务。在这一事件中，加拿大公司 AggregateIQ（AIQ）与剑桥分析公司（Cambridge Analytica）共同开发了一款名为 Ripon 的软件，利用 Facebook 数据（由剑桥分析公司利用 Facebook API 的漏洞获得）来确定选民特征，证据显示大量数据从剑桥分析公司流向 AIQ，AIQ 公司再使用这些数据帮助政治竞选团队定向投送政治类广告。2016 年英国脱欧公投前，AIQ 代表脱欧游说组织 Vote Leave 对 Facebook 用户注册的电子邮箱投放广告，影响其对脱欧的态度，类似的操作方法也出现在美国大选中。丑闻曝光后，英国信息专员办公室（ICO）判决 AIQ 公司 2000 万欧元的罚款，剑桥分析公司宣布破产清算，Facebook 由于未能对应用程序和开发者进行适当检查构成“严重违法”而对 Facebook 进行《1998 数据保护法案》上限的 50w 英镑的罚款（英国已经将 GDPR 条例引入本土，但由于调查开展的时间点在 GDPR 生效之前，Facebook 在剑桥分析事件中的判决只能适用 1998 年颁布的法案，否则 Facebook 依然会面临全球总营收额 4%的巨额罚款）。

另一个案例同样展示了 GDPR 对互联网平台数据安全的高度要求。德国一家名为 Wirtschaftsakademie Schleswig-Holstein 的学术机构在 Facebook 上运营一个粉丝页面，并通过一个名为“Facebook 观点”（Facebook Insights）的功能利用浏览器缓存（cookie）收集用户数据，其目的是向粉丝页面的管理员提供统计信息，并发布目标广告。德国数据保护局在发现该机构数据收集存在缺陷后，命令停止收集数据并停用页面。该机构否认了其在 Facebook 上处理个人数据的法律责任，否认向 Facebook 提供了有关数据处理的指示，并声称德国数据保护局应该直接对数据控制者 Facebook 采取行动，学术机构仅是 Facebook 的用户。在本案中，Facebook 只向 Wirtschaftsakademie 提供了其网站流量方面的匿名数据（通过第三方软件），即便如此，法院仍判定该学院对 Facebook 处理的非匿名数据负有共同责任，但共同责任并不意味着平等的责任，Facebook 在此案中只承担次要责任。

银行及非银金融

GDPR 优先尊重欧盟成员国法律，而银行与非银金融本身就有较为成熟的法律体系，所以相比其他行业冲击较小，主要是个人数据安全问题，其次是个人数据处理原则中的数据最小化以及数据主体七项权利。

针对银行和非银机构的个人数据安全立案调查一般源于企业公告和年报。2018 年 5 月意大利联合信贷银行（UniCredit）在罗马尼亚的分支机构由于未配备当地技术保障，导致 33.7 万条客户身份信息和地址泄露，受罚 13 万欧元；2019 年 8 月保加利亚银行（DSK）泄露 33492 名银行客户未经授权访问的个人数据，其中包含大量客户相关人员的数据（配偶、供应商、后代和担保人），被保加利亚个人数据保护委员会罚款 51.1 万欧元。

对于金融机构来说，工作组对数据主体七项权利中数据可携权、更正权、遗忘权等作出了单独解释，目的在于区别对待一些特殊场景如风控目的的信用评分。除了 GDPR 规定以外，成员国法律如丹麦《个人数据处理法》（Act on Processing of Personal Data）第 20 条中早就明确规定征信机构能够处理的数据范围以及义务。目前银行鲜有因为不为客户行使数据控制者特殊权限内信息遗忘权而被罚款的。2019 年 1 月德国 N26 银行遭到柏林数据保障局 (the Berlin Commissioner) 审查，该银行为反洗钱，将前客户的名字保留在了黑名单上，不论这些客户是否有洗钱嫌疑，未来如有新开户的需求，银行会与该黑名单进行比较，匹配得上就无法开户。后续柏林数据保障局对非法保留权限外数据处以 5 万欧元罚款，还要求采取一系列措施例如增加数据保护人员以消除以往的组织缺陷，从而改善对客户数据的保护。另一个违反了遗忘权相关案件是 2019 年 11 月法国巴黎银行罗马尼亚理财子公司由于 1 个月内没有回应是否执行客户申请删除个人财务数据而被罗马尼亚国家个人数据处理监督机构（ANSPDCP）处以约 2000 欧元的罚金。**银行与非银机构需要面临的主要是数据主体的知情权（有效同意）、处理原则中的数据最小化原则，以及限期储存原则。**法国巴黎银行捷克理财子公司曾因长期保存用户生物特征签名数据和通话录音被罚款 9704 欧元，尽管该操作已获得用户明确同意，但属地监管仍然认为该行为违反了 GDPR 第 5 条个人数据处理原则中的数据最小范围原则和限期储存原则。

总体来说，由于金融监管制度的发展早于个人数据保护，相关法律法规已经趋于完善，所以并不是个人信息保护的侧重对象，影响更多在于确保数据安全性。如在 GDPR 的框

架下，对于 250 人以上的公司，在用户数据泄露时往往因使用纯文本（而非加密）而被追责，这点同样发生在金融业。

其他实体经济行业

对于航空、能源、物流、零售、房地产等非金融、非 IT、非互联网相关产业的企业来说（以下简称“实体企业”），主要面临的是个人数据安全、数据主体的七项权利，以及个人数据处理原则的合规问题。

GDRP 高度重视实体企业信息安全方面的能力，为满足监管要求，实体企业需要进一步增加信息安全开支，包括人员培训、软硬件支出等等，其立案往往是由于公司公开披露信息引发监察部门重视。英国万豪酒店、英国航空公司、H&M 德国子公司都曾因为数据泄露遭到千万甚至上亿欧元的罚款，其中英国万豪酒店 2016 年收购喜达屋时出现客户数据泄露，同时上报不及时；英国航空公司遭到黑客攻击导致泄露客户数据；H&M 由于 IT 配置错误导致暴露员工隐私信息。

在数据主体的七项权利以及个人数据处理原则中， GDPR 更多关注数据主体知情权（有效同意）、遗忘权，个人数据处理原则中的数据最小化、限期储存原则，这几项是最容易被实体行业违反的规则。法国家乐福就被法国国家信息与通信委员会 CNIL 罚款 300 万欧元，其被认定为至少有 9 项关键违约，包括会员注册数据保护条款信息冗长、不明晰且缺少关于数据保留的关键条例；此外家乐福非法使用 cookie，过于严格地限制数据遗忘权，传输数据时没有完全透明，等等。

实体行业的数据遗忘权以及限期存储原则主要体现在“敏感数据”上，限制了实体企业对敏感数据进行数据挖掘与分析的能力。丹麦 Arp-Hansen 酒店与德国 Deutsche Wohnen SE 私人房地产公司因没有设置好删除客人/租户敏感数据(如宗教信仰、生物基因特征等) 的固定周期而分别被罚了 14.76 万欧元与 1450 万欧元。

还有一些情况涉及企业对员工、实体店铺的录像监控过当。2021 年 1 月德国线下零售商 Notebooksbilliger.de AG(NBB)因为过度监控员工工作场所被萨克森州数据保护机构 LfD Niedersachsen 罚款 1040 万欧元。LfD Niedersachsen 指出，虽然 NBB 声称安装摄像头的目的是为了安保，同时跟踪仓库货物流动，但公司应该首先考虑使用更为“温和”的手段如进行随机的物品检查，只有对特定人员在有合理怀疑的情况下才能安装摄像头在有限的时间段内进行监控，而 NBB 的视频监控不限于特定的时间，也不限于特定的员工，多数情况下被保存了 60 天，大大超过了必要时间。最后，LfD Niedersachsen 特别指出 NBB 的一些摄像头是安装在销售区域的，使得部分 NBB 客户也受到非法视频监控的影响。

严格的监管环境下，企业在供应链、销售、信息存储等方面都面临巨大挑战。首先就是是否合法收集了员工信息，荷兰某公司甚至因为仅提供生物特征辨认打卡功能而被罚款，其次是是否运用加密方式保存客户隐私信息，尤其是员工、客户群规模较大的公司，一旦发生网络安全事件（如客户数据泄露）后，仅使用纯文本储存客户敏感数据是欧洲相关部门常用的说辞。

数据监管框架如何影响企业?

从上述不同行业的案例中总结，数据监管框架的建立和完善，对企业的影响主要在三个方面：

第一，销售以及销售管理离不开对客户信息的搜集分析。但在 GDPR 的框架下，需要什么样的数据（数据最小化原则）、用途是什么（目的限制原则）、达成分析目的需要多长的时间序列（限期储存原则）、客户如何咨询数据现状（合法、公平、透明原则）以及协议是否让客户充分了解以上内容（知情权）都受到全面监管，其中互联网行业在达成“有效同意”方面格外困难，不再手到擒来的用户数据也会使定制化营销手段遭到挑战，容易触及敏感信息，不同程度降低企业的潜在利润。

第二，供应链各个环节也离不开员工等数据主体的个人数据，甚至包含一定生物特征信息（如指纹打卡等），因此在供应链监督、管理的过程中不得不考虑需要哪些数据（数据最小化原则）、如何采集（合法公开透明原则）、访问权限和数据存储技术（完整性与保密性原则）、为了实现目的需要留存多久（限期存储原则）等等。为了达到这些要求，企业可能需要增加开支（例如德国萨克森州数据保护机构认为应该增加存货盘点的频率，而非进行更严格的视频监控）。

第三，传统的信息安全管理离不开员工技术能力和软硬件的支持，企业需要增加培训以减少由于操作不当导致的数据泄露、建立规章制度以完善数据泄露的披露流程，这些都会增加企业费用(万豪酒店案例披露延迟部分源于员工在信息安全培训方面存在不足)；硬件方面可能也需要升级或转换，都会导致单笔或持续的成本开支，特别是对于技术能力较弱的企业。不过，这一因素将会利好一些提供网络安全相关服务的企业。

表 3：各行业在不同方面受到的影响总结

	通信、互联网	银行以及非银金融	实体行业
销售以及管理	高	低	中
生产与供应链管理	中	低	中
信息安全管理	高	中	高

资料来源：东方证券研究所

风险提示

跨国公司的数据监管涉及全球协调甚至在某些情况下关系到国家之间的博弈，具体政策落地与政策强度不确定性高；

监管相关机构执行力度与具体案例在社会上的伤害相比不高，从而监管执行效果不及预期。

分析师申明

每位负责撰写本研究报告全部或部分内容的研究分析师在此作以下声明：

分析师在本报告中对所提及的证券或发行人发表的任何建议和观点均准确地反映了其个人对该证券或发行人的看法和判断；分析师薪酬的任何组成部分无论是在过去、现在及将来，均与其在本研究报告中所表述的具体建议或观点无任何直接或间接的关系。

投资评级和相关定义

报告发布日后的 12 个月内的公司的涨跌幅相对同期的上证指数/深证成指的涨跌幅为基准；

公司投资评级的量化标准

买入：相对强于市场基准指数收益率 15%以上；

增持：相对强于市场基准指数收益率 5%～15%；

中性：相对于市场基准指数收益率在-5%～+5%之间波动；

减持：相对弱于市场基准指数收益率在-5%以下。

未评级 —— 由于在报告发出之时该股票不在本公司研究覆盖范围内，分析师基于当时对该股票的研究状况，未给予投资评级相关信息。

暂停评级 —— 根据监管制度及本公司相关规定，研究报告发布之时该投资对象可能与本公司存在潜在的利益冲突情形；亦或是研究报告发布当时该股票的价值和价格分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确投资评级；分析师在上述情况下暂停对该股票给予投资评级等信息，投资者需要注意在此报告发布之前曾给予该股票的投资评级、盈利预测及目标价格等信息不再有效。

行业投资评级的量化标准：

看好：相对强于市场基准指数收益率 5%以上；

中性：相对于市场基准指数收益率在-5%～+5%之间波动；

看淡：相对于市场基准指数收益率在-5%以下。

未评级：由于在报告发出之时该行业不在本公司研究覆盖范围内，分析师基于当时对该行业的研究状况，未给予投资评级等相关信息。

暂停评级：由于研究报告发布当时该行业的投资价值分析存在重大不确定性，缺乏足够的研究依据支持分析师给出明确行业投资评级；分析师在上述情况下暂停对该行业给予投资评级信息，投资者需要注意在此报告发布之前曾给予该行业的投资评级信息不再有效。

东方证券
ORIENT SECURITIES

免责声明

本证券研究报告（以下简称“本报告”）由东方证券股份有限公司（以下简称“本公司”）制作及发布。

本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。本报告的全体接收人应当采取必要措施防止本报告被转发给他人。

本报告是基于本公司认为可靠的且目前已公开的信息撰写，本公司力求但不保证该信息的准确性和完整性，客户也不应该认为该信息是准确和完整的。同时，本公司不保证文中观点或陈述不会发生任何变更，在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的证券研究报告。本公司会适时更新我们的研究，但可能会因某些规定而无法做到。除了一些定期出版的证券研究报告之外，绝大多数证券研究报告是在分析师认为适当的时候不定期地发布。

在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，也没有考虑到个别客户特殊的投资目标、财务状况或需求。客户应考虑本报告中的任何意见或建议是否符合其特定状况，若有必要应寻求专家意见。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他投资标的的邀请或向人作出邀请。

本报告中提及的投资价格和价值以及这些投资带来的收入可能会波动。过去的表现并不代表未来的表现，未来的回报也无法保证，投资者可能会损失本金。外汇汇率波动有可能对某些投资的价值或价格或来自这一投资的收入产生不良影响。那些涉及期货、期权及其它衍生工具的交易，因其包括重大的市场风险，因此并不适合所有投资者。

在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任，投资者自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

东方证券研究所

地址： 上海市中山南路 318 号东方国际金融广场 26 楼

电话： 021-63325888

传真： 021-63326786

网址： www.dfzq.com.cn