GDPR 执法案例精选白皮书

中兴通讯数据保护合规部

数据法盟

联合发布

目 录 CONTENTS

1

引 言

2018 年 5 月 25 日，欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）正式生效，深刻地影响了欧盟乃至全球范围内个人数据保护和数字经济发展态势。立法层面，GDPR 已成为各主要国家采用或计划采用的数据保护法律法规基准，引发全球立法规则进一步融合；执法层面，GDPR 执法案例作为体现监管态势的重要参照，为跨国企业的数据保护合规工作提供风向标。

鉴于 GDPR 生效时间不长，缺乏配套的适用规范和解释，通过执法案例来补充理解数据保护相关概念、明确数据处理基本原则和数据主体权利响应相关的监管要求，可以帮助企业更好地把握 GDPR 监管脉搏，也为 GDPR 相关的理论研究人员提供丰富的案例资源。

本白皮书概述了 GDPR 生效以来的新兴趋势，从执法力度、执法依据两个维度进行分析研究，提炼 GDPR 执法重点，给出企业合规启示。核心内容来源于欧洲各国监管部门、研究机构、律所等公开信息，收录了欧洲经济区(European Economic Area, EEA) 22 个国家的立法情况（立法概况、监管机构详情），87 个典型执法案例（处罚金额、依据、时间，案件事实，违规分析以及合规启示），是体现 GDPR 执法和监管态势的较为前沿的学习和参考资料。

编者（按姓氏排列）：高瑞鑫、甘亚棋、何渊、石墨翰、王业美、吴以源、徐敏。

GDPR 新兴趋势

2

2018 年是数据保护具有里程碑意义的年份。自 2018 年 5 月 25 日欧盟《通用数据保护条款》(General Data Protection Regulation, GDPR)生效以来，深刻影响欧盟乃至全球范围内个人数据保护和数字经济发展态势。许多国家已采用或计划采用 GDPR 数据保护标准进行本国数据保护立法或完善工作，从而导致全球数据保护立法规则进一步融合。

GDPR 生效以来，三大主体（监管机构、数据主体、数据控制者）对数据保护的重视程度不断提升。

监管机构执法态势

欧洲数据保护委员会(European Data Protection Board, EDPB)在 2019 年 7 月 16 日发布其首份 GDPR 年度报告，揭示了欧洲经济区(European Economic Area, EEA)（欧盟 28 国、冰岛、挪威和列支敦士登）各国家监管机构(Supervisoty Authorities, SA)落实 GDPR 的执法态势。

1 法律框架的统一

尽管 GDPR 可以直接适用于欧盟所有成员国，但它同样要求各成员国将其转化为国内法。目前，除了希腊、斯洛文尼亚，其余 26 个国家均通过不同形式将 GDPR 纳入既有法律体系之中，同时规定了本国数据保护机构（Data Protection Authority, DPA, 又称 SA）的职权，包括但不限于发出违规警告、开展审查、限期纠正、命令删除数据、暂停向第三国传输数据、罚款。

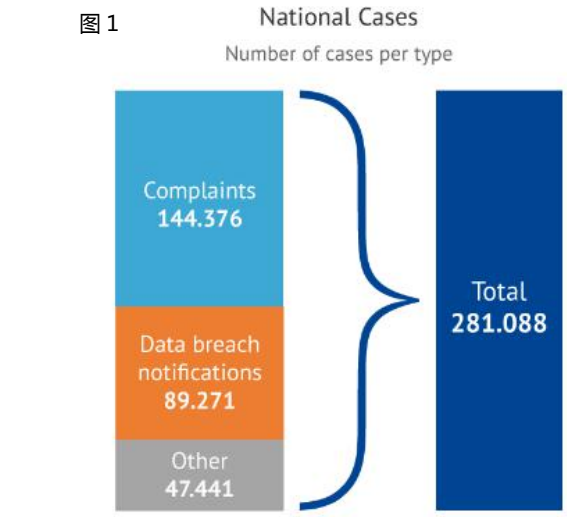
为保证欧盟整体数据保护规则的统一适用，促进各成员国 DPA 之间的合作，EDPB 批准了 16 份 WP29 工作组发布的指南，通过了 5 份指南，内容涉及 GDPR 适用地域、第 42 和 43 条下的认证及其标准、行为准则及其监督、履行合同所必需的数据处理以及数据跨境的例外情形等。

此外，EDPB 已经或正在就进行数据保护影响评估的国家名单、数据控制者与处理者间标准合同、有约束力的公司准则、通过与处理活动有关的行为守则草案、批准认证机构的认证标准等发布 “一致性意见”（Consistency opinions）。

2 处罚力度加大

来自 27 个 EEA 国家 DPA 的统计数据显示，截至 2019 年 3 月，共上报 281,088 例案件。案件主要分为 3 个主要类别，其中近半数（144,376 件）是投诉，近三分之一（89,271 件）是数据泄露通知，其余（47,441 件）涉及“其他” 问题。针对其中 164,633 件案件，63%已经审结，37%仍在进行中（图 2）。[数据来源见注 1]

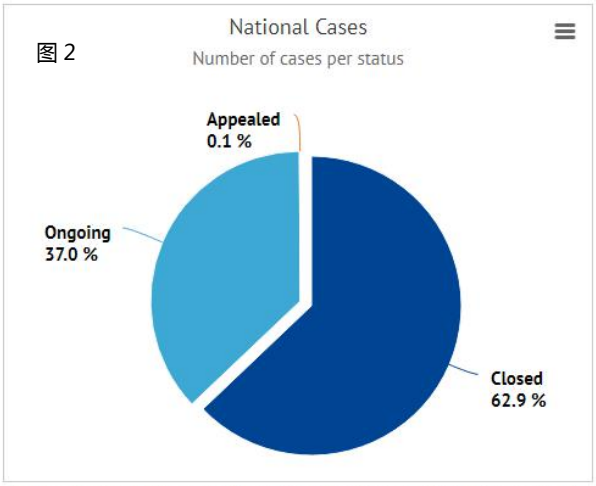
图 1



Based on information provided by SAs from 27 EEA countries
Germany: Based on information provided by The Federal and 17 Regional SAs

根据 EDPB 统计数据，自 2018 年 5 月 25 日 GDPR 生效实施以来，11 家 DPA 采取罚款监管方式共判处了 55,955,871 欧元的行政罚款。[数据来源见注 2]

图 2



Based on information provided by SAs from 27 EEA countries (Case status information provided for 164633 cases)
Germany: Based on information provided by The Federal and 11 Regional SAs

据不完全统计，截止至 2019 年 9 月 24 日，22 家 DPA 对 87 件案件共做出 373,650,857 欧元的行政处罚决定。其中，英国、法国、保加利亚、波兰、荷兰 DPA 共开出 6 件超过 50 万欧元罚款的行政处罚，最大罚单超过 2 亿欧元。经过一段时间的适应期，DPA 处罚力度明显加大，尤其进入 2019 年 7 月以来，大额罚单出现的概率明显增加。

图 3

[数据来源 注 1：1 year GDPR – taking stock, EDPB, available at: https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en]

[数据来源 注 2： First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities , available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf]

3 监管机构间的合作机制及一致性意见

GDPR 要求 EEA 国家 DPA 在涉及数据跨境的情况下密切合作，并通过使用相互帮助、联合行动、一站式合作机制进行支持。此外，为保证 DPA 适用 GDPR 的一致性，EDPB 在特殊领域发布了一致性意见，要求 EEA 各国 DPA 遵守。

为了支持 EDPB 成员之间的合作和一致性机制 ,欧盟委员会发展部与 EDPB 秘书处和 EDPB 成员定制了内部市场信息系统(Internal Market Information system, IMI)，作为中央数据库收录待处理的案件，进而启动互相帮助、联合行动和一站式机制处理程序。自 2018 年 5 月 25 日以来，30 个 DPA 在 IMI 系统中共登记了 281 起数据跨境案件。大部分未决案件来自个人投诉(194 件)，其余案例(87 件)有其他不同来源。主要涉及三个领域：数据主体权利的行使、消费者权利和数据泄露。

（1）互相帮助

互助程序允许每个 DPA 通过事先授权或调查协作等方式向其他 DPA 收集案件信息。这种互助可用于受一站式程序制约的跨境案件(作为起草决议前收集必要信息的初步阶段的一部分)，也可用于具有跨境特征的国家案件。

互相帮助分为正式互助和非正式互助两类。被要求的 DPA 有 1 个月的法定答复期限的情况下可以使用正式互助。被要求的 DPA 没有任何法定期限的情况下可以使用非正式互助。自 2018 年 5 月 25 日以来，来自 18 个不同 EEA 国家的 DPA 触发了 444 项(正式和非正式)互助请求。在 444 项互助请求中，有 353 项在 23 天内发出了答复。其余 91 起案件仍在进行中，尚未得到 DPA 的答复。

（2）联合行动

GDPR 允许不同成员国的 DPA 开展联合调查和联合执法措施。联合行动可用于受一站式程序制约的跨境案件(作为起草决定前收集必要信息的初步阶段的一部分) ,也可用于包括跨境部分的国家案件。自 2018 年 5 月 25 日至 2019 年 1 月 31 日，没有发起任何联合行动。

（3）一站式机制

一站式机制适用于跨境案件，即数据控制者或数据处理者在不止一个成员国设有机构，或者数据处理活动对不止一个成员国的个人产生重大影响。

在一站式机制下，将产生一个主导机构负责领导合作程序，就案件展开调查。在这一调查阶段，它可以通过相互帮助从其他 DPA 处收集信息，或者在各国家法律可预期的情况下进行联合调查。

IMI 系统提供不同的程序来处理一站式案件:

1.非正式磋商程序；

2.主导机构向相关 DPA 提交草案或修订草案；

3.相关 DPA 审议和 EDPB 的最终一站式决定。

如有必要，主导机构可以发起与所有相关 DPA 的非正式沟通，以收集信息并准备相关草案。主导机构完成调查后，需要准备一份草案，并将其传达给相关 DPA。DPA 可以反对该草案，该反对意见要么导致草案的重新修订，要么触发理事会的争端解决机制。

自 2018 年 5 月 25 日以来，来自 14 个 EEA 国家的 DPA 启动了 45 个一站式服务程序。这 45 个程序处于不同阶段：23 个处于非正式磋商阶段，16 个处于草案阶段，6 个处于最终决定阶段。这些最后的一站式决策涉及个人权利的行使（如被遗忘权）、数据处理的合法性依据和数据泄露通知。

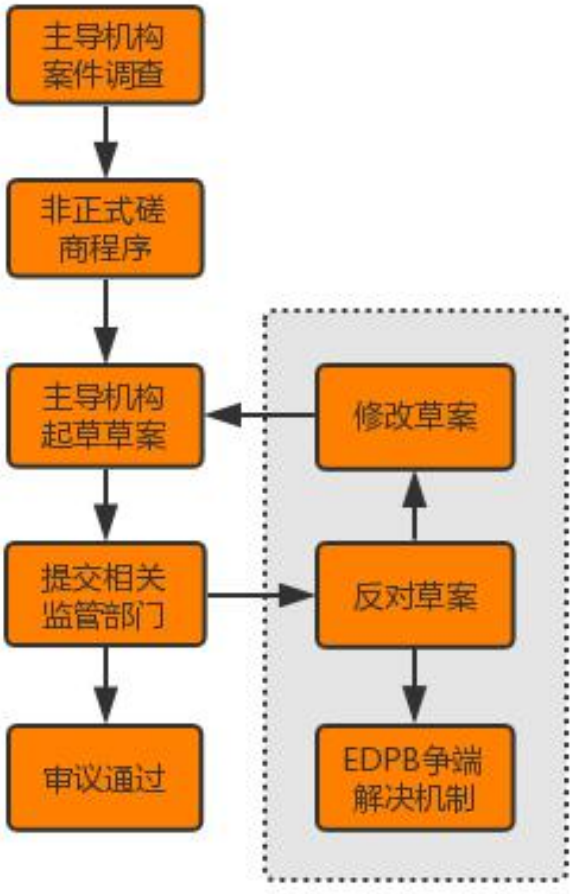


图 4：一站式服务机制流程图

（4）一致性机制

为保证 DPA 适用 GDPR 的一致性，EDPB 在特殊领域发布了一致性意见，要求 EEA 各国 DPA 遵守。在通过有关数据保护影响评估的国家名单、数据控制者与处理者间标准合同等决议之前，各国 DPA 必须事先征求 EDPB 意见。

自 2018 年 5 月 25 日以来，EDPB 通过了 28 项关于受数据保护影响评估制约的国家处理清单的意见和 1 项关于金融监管机构(欧洲经济区内和欧洲经济区外)之间个人数据传输行政安排草案的意见。

目前有 3 个正在进行的程序，涉及具有约束力的公司规则、数据控制者和数据处理者之间的标准合同草案以及 GDPR 和《欧盟电子隐私条例》(EU ePrivacy Regulation, ePR)之间的相互作用，特别是关于国家 DPA 的权限。

在 DPA 不遵循 EDPB 的一致性意见的情况下，EDPB 作为争端解决机构进行干预并做出具有约束力的决定。

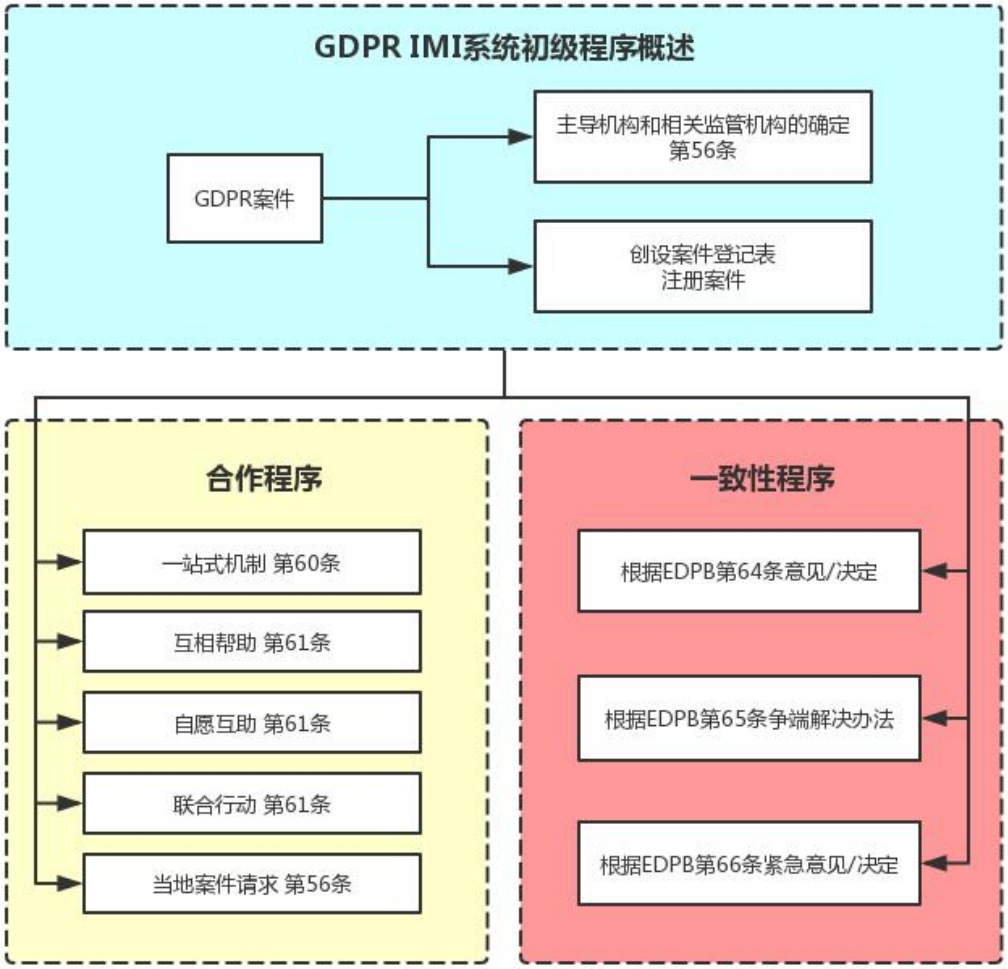


图 5：GDPR IMI 系统初级程序概述

4 2019-2020 工作计划

2019 年 2 月 19 日，EDPB 发布了为期两年（2019-2020）的工作计划，未来 EDPB 将聚焦数据主体权利、数据控制者和数据处理者概念及合法利益，更加关注专业领域和技术。2019-2020 工作计划主要包括以下几方面内容。

（1）数据主体权利

EDPB 将为数据主体的访问权、被遗忘权、拒绝权等权利的实现以及儿童数据保护制定指南。此外，还将提供关于在选举中使用个人数据的声明。

（2）数据控制者和数据处理者

EDPB 将为数据控制者和数据处理者的概念、数据控制者的合法利益制定指南。

（3）ePR 和在线服务

EDPB 将为 ePR 和 GDPR 之间的相互作用发布一致性指导意见；为社交媒体用户制定指南；为使用在线服务合同制定指南；以及为联网车辆、区块链、人工智能和数字助手、视频监控、搜索引擎、注销、通过设计和默认方式保护数据等新领域、新技术制定指南。

（4）跨境传输

EDPB 将对为行政合作目的的公共机构之间的数据跨境制定指南。此外，EDPB 还将继续根据《商标保护法》规定的跨境转移的标准合同条款、处理者的标准合同条款、跨境转移的临时合同条款以及具有约束力的公司规则提供一致性意见和决定。

（5）其他

EDPB 将为 GDPR 管辖范围制定指南；为数据泄露通知提供指导意见；以及为 DPIA 清单提供一致性意见和决定。

个人权利意识提高

保护个人的基本权利是 GDPR 的重要目标。随着 GDPR 执法的深入，公众对数据保护规则及个人权利的了解度有了很大的提升。向 DPA 咨询 GDPR 和提出申诉的人日益增多，来自 27 个 EEA 国家 DPA 的统计数据显示，截至 2019 年 3 月共上报了 281,088 例案件，其中近半数（144,376 件）是投诉。同时，非营利组织代表个人发起的申诉也开始出现。

企业合规投入增加

在资源投入方面，越来越多的企业在人力、资金等方面加大投入。根据国际隐私专业人士协会(International Association of Privacy Professionals, IAPP)2019 年 7 月发布的数据显示，目前在 28 个欧盟成员国的 12 个国家中，约有 376,306 个组织注册了 DPO。据估计，整个欧洲总共有 500,000 个 DPO 实际注册。根据 IAPP 和安永(Ernst & Young, EY)发布的 2018 年隐私治理报告，每个组织的平均支出将达到约 300 万美元，支出主要分布在：内部人员（33%）、外部法律顾问（18%）、咨询（15%）、员工培训（12%）以及新技术解决方案的开发（22%）。

在数据保护合规治理方面，企业也在积极改善数据管理的安全性，降低不必要的合规风险，维护与客户和商业伙伴之间的良好信任关系。在数据处理透明度方面，企业也在探索如何在个人权利保障与商业运营之间达成良性平衡关系，尽可能满足数据主体的权利请求。

GDPR 执法重点

3

GDPR 执法重点从执法力度国别性差异和执法依据两个维度进行分析。

执法力度国别分析

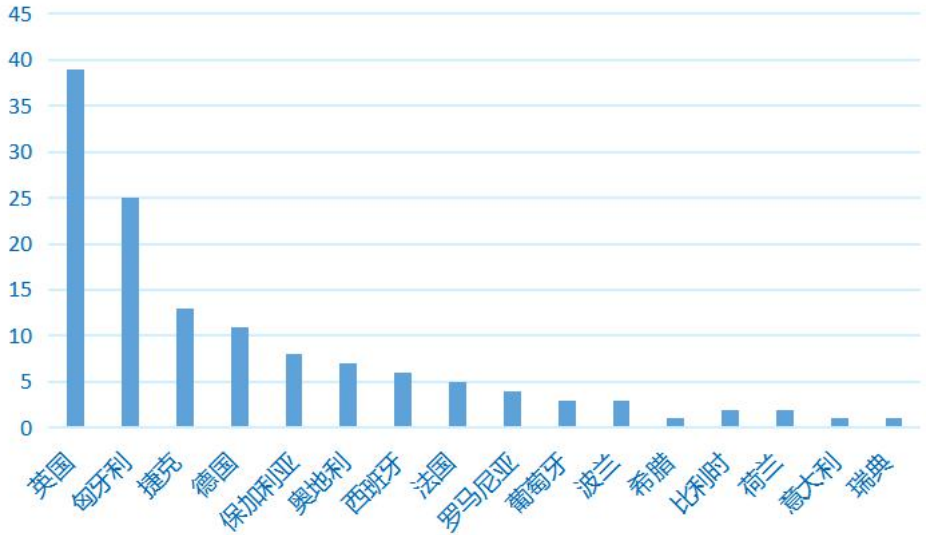


图 6：欧洲国家数据保护执法案件数量对比图（统计限于重点欧洲国家）

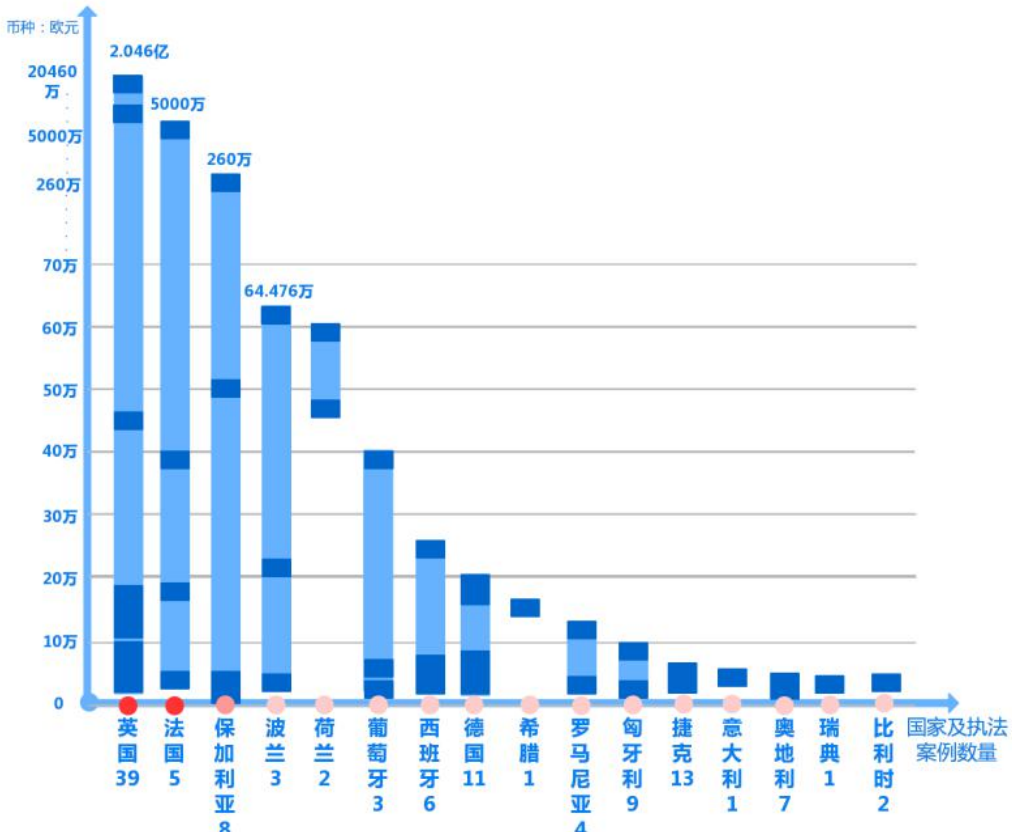


图 7：欧洲国家数据保护执法金额对比图（统计限于重点欧洲国家）

图例说明：浅蓝色柱状部分表示罚款金额分布范围，深蓝色柱条表示罚款金额较为集中的部分

（1）英国

英国数据保护监管机构（ICO）有记录的处罚案例共计 112 起，自 GDPR 生效以来的执法案例共计 71 起。涉及的企业/组织类型：市场营销（18 起），金融保险和信贷（8 起），一般业务（7 起），房地产服务（6 起），健康医疗（5 起），零售与制造商（4 起），刑事司法领域（4 起），交通和休闲（3 起），互联网科技和网络（2 起），中央政府（2 起），地方政府（2 起），媒体（1 起），协会组织（1 起），政治（1 起），慈善与志愿者（1 起），教育与儿童托管（1 起）。

其中被处以罚款的有 39 起，下发执行整改通知的有 19 起，被检方起诉的有 12 起，签署责任承担承诺函的有 1 起。英国近期两起执法案例创 GDPR 生效以来最高罚款记录：①英国航空公司因违反 GDPR 被罚 2.046 亿欧元（约合 15.94 亿元人民币）；②万豪集团被罚 1.1 亿欧元（约合 8.57 亿元人民币）。英国数据保护执法力度之大、之严由此可见一斑。

（本报告仅选取英国执法案例中两起“天价罚单”进行详细分析）

（2）法国

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来的执法案例共计 5 起，最高的一笔执法金额是对谷歌公司处以 5000 万欧元（约合 3.9 亿元人民币）的罚款，最低的一起处罚金额为 2 万欧元（约合 15.6 万元人民币）。

（3）德国

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来的执法案例共计 11 起，最高的两笔执法金额分别是：①对一家网络公司处以 20 万欧元（约合 156.2 万元人民币）罚款；②对交易服务平台 Delivery Hero 处以 19.5407 万欧元（约合 152.6 万元人民币）；最低的一起处罚金额为 118 欧元（约合 922 元人民币）。

（4）匈牙利

根据匈牙利数据保护监管机构（NAIH）官网显示，匈牙利 2019 年数据保护执法案例 20 起，2018 年 18 起，2017 年 25 起，2016 年 11 起，2015 年 20 起，2014 年 18 起，2013 年 42 起，2012 年 11 起。其中，自 GDPR 生效以来的执法案例共计 25 起。

匈牙利数据保护执法金额并不像英、法、德等国处罚力度那么大，大部分案件处罚金额在 1560 欧元（约合 1.2 万元人民币）至 1 万欧元（约合 7.8 万元人民币）范围内浮动，匈牙利目前最高的一笔处罚金额为 9.2146 万欧元（约合 72 万元人民币）。

总体上来看，匈牙利数据保护执法动作较为频繁，但执法金额相对平缓。

（本报告选取 GDPR 生效以来的 9 起执法案例进行分析）

（5）保加利亚

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来共计执法 8 起，最高的一笔执法金额是对国家税务局处以 260 万欧元(约合 2038.4 万元人民币)的罚款，最低的几起处罚金额均为 500 欧元（约合 3920 元人民币），这几笔处罚均属于未响应或未充分响应单个数据主体的行权请求。

（6）波兰

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来的执法案例共计 3 起，最高的一笔执法金额是近期对购物网站 Morele.net 处以 64.478 万欧元(约合 503.6 万元人民币) 的罚款，其次是对数字营销公司 Bisnode 处以 21.9538 万欧元（约合 171.5 万元人民币）的罚款，最低一笔处罚金额为 1.295 万欧元（约合 10.1 万元人民币）。

波兰数据保护执法案件虽不多，但执法力度相对较大。

（7）荷兰

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来的执法案例共计 2 起，执法金额分别为对某医院处以 46 万欧元(约合 359.3 万元人民币)和对 Uber Technologies,Inc(优步) 处以 60 万欧元（约合 468.6 万元人民币）的罚款。

此外，值得注意的是，荷兰早在 2017 年就对 Facebook 违反数据保护法发布了整改通知——Facebook 违反荷兰数据保护法，未向用户提供有关其个人数据被使用的充分信息；此外，Facebook 未经用户明确同意使用用户的敏感个人数据，如与性偏好有关的数据被用于个性化广告投放。Facebook 已根据整改通知做出整改。荷兰数据保护执法走在了欧盟层面（GDPR）的前面。

荷兰数据保护执法案件虽然不多，但执法力度相对较大。

（8）葡萄牙

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来的执法案例共计 3 起，最高的一笔执法金额是对 Barreiro 医院处以 40 万欧元（约合 312.4 万元人民币）的罚款，最低的一起处罚金额为 2000 欧元(约合 15621 元人民币）。

（9）西班牙

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来的执法案例共计 6 起，最高的一笔执法金额是对足球联盟 Professional Football League (LaLiga)处以 25 万欧元（约合 195.3 万元人民币）的罚款，最低的一起处罚金额为 5000 欧元（约合 3.9 万元人民币）。

（10）奥地利

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来的执法案例共计 7 起，最高的一笔执法金额是对一家医疗公司处以 5 万欧元（约合 39 万元人民币）的罚款，最低的一起处罚金额为 300 欧元（约合 2343 元人民币）。

（11）捷克

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/）及捷克数据保护监管机构（OPDP）官网发布的 2018 年年度报告的统计数据显示，GDPR 生效以来的执法案例共计 13 起，最高的一笔执法金额是对一家网络购物商城处以 5.8 万欧元（约合 45.3 万元人民币）的罚款，最低的一起处罚金额为 194 欧元（约合 1515 元人民币。

（12）比利时

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来的执法案例共计 2 起，分别是对某店主处以 1 万欧元（约合 7.8 万元人民币）的罚款，以及对比利时市市长处以 2000 欧元（约合 15621 元人民币）的罚款。

比利时数据保护执法力度相对较低。

（13）瑞典

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/）及汤森路透的统计，瑞典的数据保护执法案例查询到 1 起，即对一所学校使用人脸识别技术来记录学生考勤处以 1.8630 万欧元（约合 14.5514 万元人民币）罚款。鉴于面部识别信息属于 GDPR 项下的特殊类型个人数据，且该学校违反 GDPR 的基本原则收集、使用未成年人个人数据。虽然该罚款金额相对较低，但个例不能表明瑞典的数据保护执法力度普遍偏低。

（14）希腊

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/）及汤森路透对希腊数据保护执法案例的统计，GDPR 生效以来查询到执法案例 1 起，即对普华永道非法处理员工个人数据处以金额 15 万欧元（约合 117.2 万元人民币）的罚款。

（15）罗马尼亚

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/），GDPR 生效以来的执法案例共计 4 起，最高的一笔执法金额是对 UNICREDIT 银行处以 13 万欧元（约合 101.5 万元人民币）的罚款，最低的一起罚款金额为 2500 欧元（约合 2 万元人民币）。

（16）意大利

根据 GDPR 执法跟踪的统计（http://www.enforcementtracker.com/）及汤森路透对意大利数据保护执法案例的统计，GDPR 生效以来查询到执法案例 1 起，执法金额为 5 万欧元（约合 39 万元人民币）。

（17）其他国家

此外，对于其他欧洲国家，包括挪威、马耳他、立陶宛、塞浦路斯、拉脱维亚、丹麦，从执法案例数量及处罚金额两个维度考察，数据保护执法力度相对较大的为挪威和丹麦，其余四个国家数据保护执法力度较低。

图8：GDPR执法案件处罚依据数量分布图

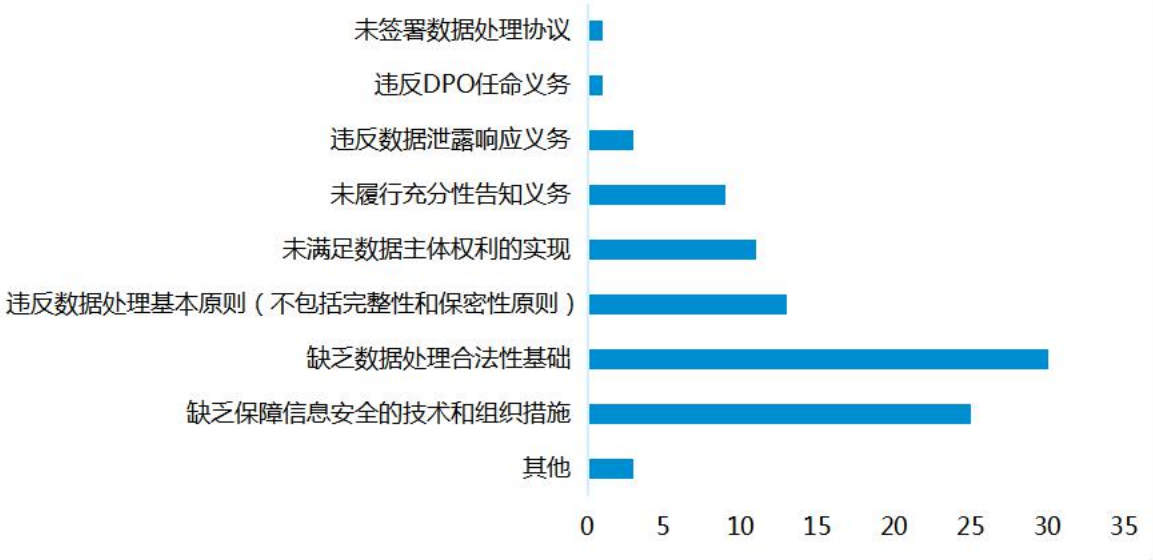
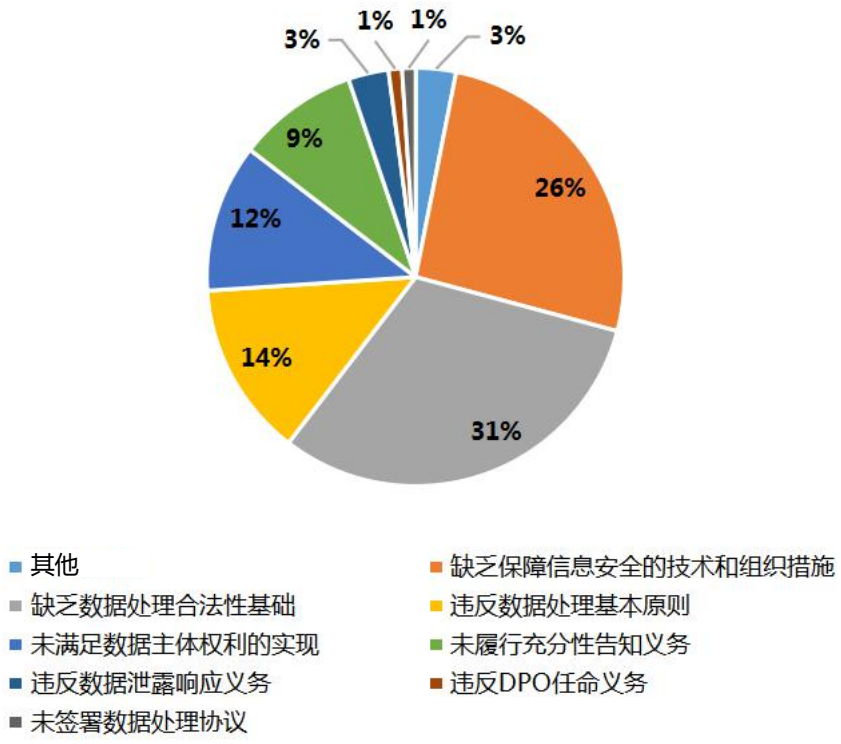


图9：GDPR执法案件处罚依据种类占比图



从 GDPR 执法案件的处罚依据上分析，监管机构的高频度执法依据主要是 GDPR 第 5、6、12、13、14、15、16、17、28、32、33、34、37 条，归纳总结各个法条内容，得出以下八项处罚依据，具体情况可参见表 1 处罚依据条款及内容对应表。

序号	高频执法依据条款	所对应处罚依据内容
1	Art. 5 GDPR	违反数据处理基本原则
2	Art. 6 GDPR	缺乏数据处理合法性基础
3	Art. 12,13,14 GDPR	未履行充分性告知义务
4	Art. 15,16,17 GDPR	未满足数据主体权利的实现
5	Art. 28 GDPR	未签署数据处理协议
6	Art. 32 GDPR	缺乏保障信息安全的技术和组织措施
7	Art. 33,34 GDPR	违反数据泄露响应义务
8	Art. 37 GDPR	违反 DPO 任命义务

表 1：处罚依据条款及内容对应表

监管机构的执法重点在于 GDPR 第 5 条中的数据处理的基本原则与第 6 条数据处理的合法性基础。其中，数据处理的合法性基础的缺失（合法性原则）的执法力度最为显著。在我们搜集的 87 个案例中，8 个案例是依照多类别处罚依据执法（其中 7 个有 2 个处罚依据，1 个有 3 个处罚依据）。所有的处罚依据中，有 30 个是因为缺乏数据处理的合法性基础而被罚，占比 31%。另外，数据处理的安全性（完整性与保密性）也是执法机构关注的重点，案例处罚依据数量为 25 个，占比 26%。其他比较显著的是违反数据处理的其他基本原则，以及数据主体权利响应和充分性告知义务的履行，占比分别在 14%、12%、9%。详情请参考图 8、图 9。

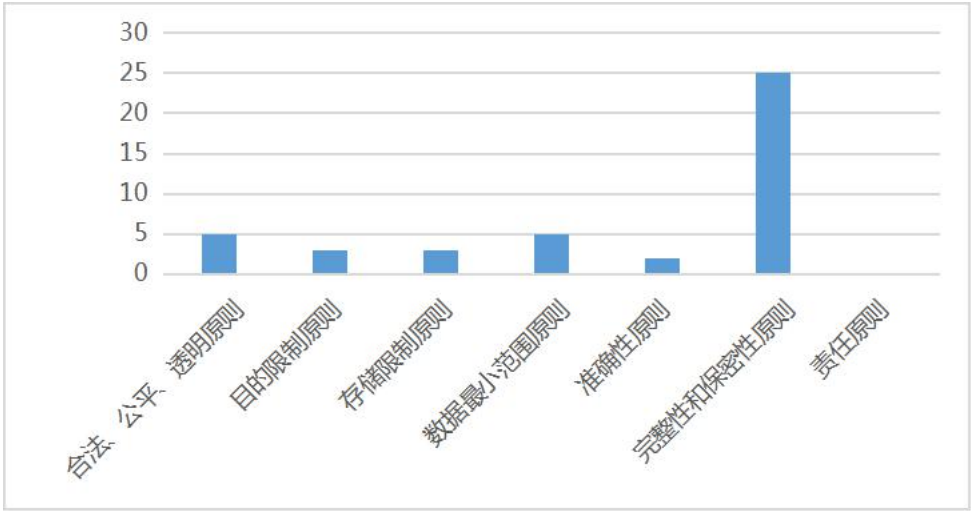


图 10：违反数据处理基本原则分布图

GDPR 中规定了数据处理的七大原则，在这些原则中，触犯频率最高的原则是完整性和保密性原则，即缺乏相应的技术组织措施保障数据处理安全性，其他基本原则的违反情况较为平均。详情请参考图 10。

GDPR 合规启示

4

结合 GDPR 规定及欧盟地区各个国家监管机构的执法案例，企业在处理（包括但不限于收集、使用、转移、披露）个人数据时应当遵守数据处理七大基本原则，并且应当充分保障数据主体权利的实现。

根据 GDPR 执法依据重点分析，企业应当尤其注意遵守**完整性和保密性原则、合法、公平和透明原则以及数据最小范围原则**，充分保障数据主体**访问权、被遗忘权**的实现。

根据 GDPR 执法力度国别分析，**英国、法国、保加利亚、波兰**处罚力度大，**英国、匈牙利、捷克、德国**监管机构处罚动作频繁。企业需要重视在上述国家的数据保护合规治理工作。

遵守数据处理基本原则

1 合法、公平和透明原则

企业处理个人数据应当获得数据主体同意或具有其他合法性基础。未经同意或不具有其他合法性基础，不得处理（包括但不限于收集、使用、转让、披露）个人数据。

企业应当以简单明了、透明以及易获得的形式将 GDPR 第 13 条和第 14 条要求提供的信息提供给数据主体，特别注意相关信息不应过度分散，确保用户能够通过相对容易的操作访问其个人数据相关信息。

（1）使用“同意”作为合法性基础的局限性

“同意”需要符合自愿、自由要求。双方地位不平等将导致同意因欠缺自愿要素而失去效力。尤其在雇佣关系中，需谨慎应用“同意”。再次，“同意”需要符合明确、具体要求，针对不同的处理行为、处理目的获取相应的“同意”，禁止一揽子“授权同意”。从公司的角度出发，建议仅在其他合法性基础不适用的情况下才将“同意”作为合法性基础。

（2）间接来源数据的授权合法性核查

间接收集、使用个人信息时，应核查并确认数据提供方取得数据主体授权的情况及范围。

（3）履行公共利益职责处理个人数据

当进行履行涉及公共利益的职责所必要的数据处理时，应符合相关国家的具体规定，并对处理行为设立更为精细的具体要求和其他措施来确保数据处理的合法与公平。

（4）电子邮件发送场景中第三方披露问题

向第三方披露个人信息，应当取得数据主体的同意或具有其他合法性基础。在发送电子邮件的场景中，如果收件人彼此之间没有互相披露的合理性理由，企业应当采取密送方式保护每个收件人的个人邮箱地址不向其他第三人披露。

在员工设置个人工作账户密码时提示其设置密级较高的密码，避免公司所有员工共享涉及客户个人数据的企业电子邮件等类似工作账户。

（5）新技术风险评估

新技术投入使用时，应当重视风险评估合规工作。形式主义的风险评估并不能被监管部门认可，风险评估必须包含对处理目的必要性及相称性的评估和说明、对数据主体权利和自由存在的风险的评估等内容。

2 目的限制原则

企业应当遵守目的限制原则，基于具体、明确、合法的目的收集个人数据，且随后不得以与该目的相违背的方式进行处理。

3 最小范围原则

企业应当遵守数据最小化原则。处理个人数据应当与目的相称，收集、处理的个人信息应当是充分的、相关的，并且与处理目的相关。

❖ 举例：视频监控设备

公司安装视频监视设备应当是出于确保人员和财产安全的目的，应避免对员工进行持续和永久的拍摄，禁止侵犯员工个人隐私。

❖ 举例：人脸识别等生物特征数据

对于人脸识别等生物特征数据的使用持谨慎态度。如果生物特征数据用于出勤统计目的，则其处理的合法性往往不被监管机构认可。因为有多种风险性更低的方式可以用于实现该目的。因此，只有在用其他方法无法以令人满意的方式实现处理目的时，才可以考虑使用此类敏感数据，否则存在较大的合规风险。

4 准确性原则

企业应确保其处理的数据保持适时地更新，并采取一切合理的措施确保错误数据被及时清除或更正。

5 存储限制原则

企业应当遵守存储限制原则，个人数据以可识别形式存储的，其存储期限不能长于完成处理目的所需的时间。这意味着，当不再需要个人数据时，通常必须将其删除或匿名化处理。此外还需要注意各成员国关于数据留存期限的具体法律规定。

6 完整性和保密性原则

数据处理应当以确保个人数据的适当安全性的方式进行，包括采取适当的技术和组织措施以保护数据免遭未经授权或非法处理以及意外的丢失、销毁或破坏。发生数据泄露事件，企业应当及时采取措施消除风险，在规定时间内报告监管部门，并告知受影响的数据主体数据泄露相关情况。

（1）采取充分保障信息安全的技术和组织措施

❖ 日常管理及定期检查

企业应当在日常的经营活动中重视并定期开展合规性检查，在系统安全方面采取更多、有效的保护措施。

❖ 兼收并购中进行数据合规尽职调查

企业须在兼并和收购背景下重视数据共享的重要性，将其视为潜在的“优先事项”。如果标的公司的业务涉及个人数据，那么企业应当把数据合规尽职调查放到与其他资产尽职调查同等重要的地位，遵守 GDPR 治理和责任要求，从而避免日后发生数据泄露事件给企业带来巨额损失。

❖ 产品开发与测评

在开发移动应用程序时，应当采取安全保护措施，重视产品的安全性和保密性。在投入使用前，应当进行充分测试，防止重大安全漏洞。适当的安全措施包括但不限于评估个人数据是否以受保护的格式存储，是否通过安全连接对数据共享进行加密以及应用程序是否应用了受信任的证书等。

❖ 敏感或特殊类型个人数据特殊保护

企业应当对敏感或特殊类型个人数据进行加密等保障措施，及时识别风险，并采取措施防范风险。对于儿童应当给予特殊保护，提供更高的保护力度，例如采取加密、严格管控访问权限等措施。

❖ 访问权限控制

企业应当采取措施确保任何对个人数据享有访问权限的雇员或其他授权主体非经指示不得处理这些数据。企业应当在两方面采取充分的访问权限安全保障措施：一是定期检查访问记录，及时发现风险信号，对于未经授权查阅数据的行为进行整治。二是采取多重验证访问身份的机制，良好的安全性要求身份验证至少涉及两个因素，例如可以使用密码并结合员工通行证来验证访问身份。

（2）履行数据泄露响应义务

❖ 保存数据泄露处理日志

企业应当在日常管理中建立相对完善的数据管理制度，采用日志系统等安全保障措施记录数据处理行为，预警风险信息。

❖ 第三方委托结果验收

委托第三方处理数据泄露事件时，企业应当验证委托方应对数据泄露事件的行为和结果的有效性。

❖ 数据泄露事件报告

发生个人数据泄露事件时，企业应当采取及时调查、主动上报、积极止损的方式，与监管机构保持良好密切的沟通，有助于将影响控制在尽可能小的范围内。企业应当自发现之时起 72 小时内，报告监管机构，及时通知个人数据泄露情况可能会为接下来的监管调查提供有力证明，同时也是监管机构做出处罚决定的考虑因素之一。在大规模数据泄露事件中，企业应当告知数据主体数据泄露相关信息。

7 责任原则

❖ 保存数据处理活动记录

企业应当建立数据处理日志系统，保存数据处理活动的记录，并定期检查数据处理活动日志，及时预警风险信息。将数据处理活动记录作为企业数据保护合规的运行结果记录与证据。

❖ 任命数据保护专员

当企业作为数据控制者或数据处理者，核心业务由数据处理组成或涉及到 GDPR 规定的特殊类型数据或与犯罪记录、违法行为有关数据组成时，应当任命数据保护专员（DPO）。

❖ 与数据处理者签署数据处理协议

企业与第三方主体共同处理或委托第三方处理个人数据，应当签订数据处理协议。数据处理协议内容应当包括处理行为的内容和期限、性质和目的、个人数据的类型和数据主体的种类、采取保障信息安全的技术组织措施的细节以及数据控制者/数据处理者的权利和义务。

对数据处理者处理行为及责任不清楚，并不能成为免除数据控制者签署数据处理协议责任的抗辩理由。在不清楚数据处理者处理行为的情况下进行的数据处理活动，具有非常高的合规风险。

充分保障数据主体权利的实现

企业应当对数据主体履行充分性告知义务，保障数据主体的知情权。对于数据主体行使访问权、更正权、删除权（被遗忘权）、限制处理权、数据可携权、拒绝权等权利时，企业不得拖延，应及时响应数据主体的行权要求。

1 知情权

（1）直接收集个人数据

企业收集、处理个人数据应遵守合法、公平和透明原则，告知数据主体关于数据收集类型、处理目的、合法性基础、个人数据控制者的身份和联系方式、存储期限（在无法确定具体时间的情况下应提供确定存储期限的标准）、安全保障措施、数据主体权利等信息。

采用摄像监控方式的，应当在监控区域设置提醒，标识监控范围，履行告知义务。

（2）公开渠道收集个人数据

企业从公开渠道获取数据主体信息用于商业目的时，应当向数据主体履行告知义务。企业应当采用一切可行的方式履行告知义务。只有在穷尽所有可能办法而无法实现时，才能采用公示告知的方式。

2 访问权

当数据主体行使访问权时，企业应当在法律规定期限内（一个月内）响应数据主体的行权要求，特殊情况下可以延长至两个月。

3 更正权

当数据主体要求更正错误个人数据时，企业应当及时响应数据主体行权要求，及时更正与其有关的错误数据。

4 删除权（被遗忘权）

当数据主体撤回同意或当个人数据处理已不必要情况下，数据主体提出删除其个人数据的请求时，企业应及时采取删除措施，清除与其相关的个人数据。

5 限制处理权

当数据主体对个人数据的准确性提出质疑、数据处理违法情况下数据主体要求限制数据使用或数据主体行使拒绝权的情况下，数据主体有权限制企业的数据处理行为。

除数据存储外，在数据处理受限制的情况下，仅经数据主体同意后企业才能处理数据，除非出于诉讼程序需要、保护其他自然人、法人权利，或为欧盟或成员国重要公共利益而处理数据。数据处理受限制的情况下，企业应当在限制处理落实前通知数据主体。

6 数据可携权

当数据处理是基于数据主体同意或合同约定合法性基础，或数据通过自动化方式进行处理的情况下 ,提供个人数据的数据主体有权向企业要求提供结构化、通用化和可机读的与其有关的个人数据。同时，数据主体有权将这些数据转移给其他数据控制者，原数据控制者不得进行阻碍。

7 拒绝权

为营销目的处理个人数据的，应当征得数据主体同意。当数据主体明确拒绝为广告营销目的处理其个人数据，企业不得向其推送广告。

5

欧洲主要国家执法典型案例

5.1 英 国

立法概况

- Access to Health Record Act 1990
- Access to Medical Reports Act 1988
- Crime (Overseas Production Orders) Act 2019
- Data Protection Act 2018
- Digital Economy Act 2017, UK STATUTE 2017 C. 30
- Freedom of Information Act 2000
- Health and Social Care (National Data Guardian) Act
- Identity Documents Act 2010
- Investigatory Powers Act 2016
- Regulation of Investigatory Powers Act 2000

监管机构

Information Commissioner's Office (ICO, DPA)
网址：https://ico.org.uk/
电话: 0303 123 1113
传真: 01625 524510

Wales office：
电话：0330 414 6421
Email: wales@ico.org.uk

Northern Ireland office：
电话：028 9027 8757 / 0303 123 1114
E-mail: ni@ico.org.uk

Scotland office：
电话: 0303 123 1115
E-mail:
Scotland@ico.org.uk

01 英国航空公司数据泄露事件

- **拟处罚金额**
  2.04 亿欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/7/8

案件事实概述

2018年6月起英国航空公司网站发生了数据泄露事件，9 月英国航空公司向 ICO 通报该数据泄露事件。

该事件导致约 50 万名英航乘客的个人信息被泄露。在该事件中，用户流量被移转到虚假网站，攻击者通过这个虚假网站收集了客户详细信息，包括**客户个人信息和银行卡信息，如姓名、地址、邮箱，以及信用卡的号码、有效期和背面的验证码（CVV）等**。事件爆发后，英国航空公司配合 ICO 调查并对安全系统进行整改，获得向 ICO 提出有关拟议调查结果和制裁的陈述机会。

此外，ICO 作为牵头监督机构，代表其他欧盟成员国数据保护机构调查此案件。它还与其他监管机构联络。根据 GDPR“一站式服务”规定，受影响的欧盟数据保护机构也将有机会对 ICO 的调查结果发表评论。

针对此次事件，ICO 拟对英国航空作出 2.04 亿欧元的罚款决定。

违规分析

英国航空公司缺乏保障信息安全的技术和组织措施。

合规启示

1. 企业应当在日常的经营活动中重视并定期开展合规性检查，在系统安全方面采取更多、有效的保护措施；

2. 应对数据泄露事件时，事前形成相对完善的数据管理制度，采取防护措施，事中采取及时调查、主动上报、积极止损的方式，与监管机构保持良好密切的沟通，并将数据泄露的事实告知数据主体，有助于将影响控制在尽可能小的范围内。

02 万豪集团数据泄露事件

- **拟处罚金额**
  1.1 亿欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/7/9

案件事实概述

2018 年 11 月，万豪国际集团公开披露其旗下喜达屋酒店客房预订系统数据泄露事件。该事件导致 3.39 亿酒店客户信息被黑客窃取，涉及到 3000 万来自 31 个欧洲经济区（EEA）国家的居民，其中包括 700 万英国居民。

万豪国际在 2016 年 9 月收购了喜达屋酒店。据 ICO 调查，喜达屋酒店客房预订系统因黑客攻击导致的数据漏洞自 2014 年 7 月起便存在，直到 2018 年才发现此漏洞。

针对此次事件，ICO 拟对万豪国际集团作出 1.1 亿欧元的罚款决定。

违规分析

1. 收购喜达屋酒店时未作充分的尽职调查发现系统漏洞

2. 在保证酒店系统安全方面，万豪国际缺乏保障信息安全的技术和组织措施

合规启示

1. 企业须在兼并和收购背景下重视数据共享的重要性，将其视为潜在的“优先事项”。只要标的公司的业务涉及数据，则应当把数据合规尽职调查放到与公司其他资产尽职调查同等重要的地位，遵守 GDPR 治理和责任要求，从而避免日后发生数据漏洞给企业带来的巨额损失；

2. 企业应当在日常的经营活动中重视并定期开展合规性检查，在系统安全方面采取更多、有效的保护措施；

3. 应对数据泄露事件时， 事前形成相对完善的数据管理制度，采取防护措施，事中采取及时调查、主动上报、积极止损的方式，与监管机构保持良好密切的沟通，并将数据泄露的事实告知数据主体，有助于将影响控制在尽可能小的范围内。

5.2 法 国

立法概况

- Data Protection Act (Consolidated 2018)
- Protection of Personal Data and Amending Act
- Regulation on Implementation of Biometric Authentication Systems

监管机构

Commission Nationale de l'Informatique et des Libertés (CNIL, DPA)
网址: https://www.cnil.fr/
电话：+33 (0)1.53.73.22.22
传真：+33 (0)1.53.73.22.00

Google

01 Google 定向广告推送事件

- **处罚金额**
  5 千万欧元
- **处罚依据**
  Art. 4 nr. 11 GDPR
  Art. 5 GDPR
  Art. 6 GDPR
  Art. 13 GDPR
  Art. 14 GDPR
- **处罚时间**
  2019/1/21

案件事实概述

1. 谷歌向用户提供的信息（例如数据处理目的，数据存储时间或用于广告个性化的个人数据类别），过度分散于多个文件中，需要用户经过五六个步骤才能访问

2.对于广告个性化投放的数据处理目的、基于不同目的收集和处理的数据类别的描述过于笼统和含糊。用户无法据此了解谷歌到底适用用户的同意还是根据公司自身利益来处理数据。Google 还预先勾选了广告个性化的显示框，但是，根据 GDPR 的规定，只有用户明确的肯定行动（例如勾选未预先勾选的显示框），同意才是明确的；

3.谷歌要求用户必须完全同意隐私政策中的服务条款和数据处理条款，而非区分各种不同目的（如个性化广告或语音识别等）来同意各项条款。

违规分析

1.违反透明性原则，用户无法轻易访问 Google 提供的信息。

谷歌在用户访问个人数据上缺乏透明度，一方面，用户无法了解谷歌“大规模的、侵入性的”数据处理达到了什么样的程度；另一方面，即使是谷歌已经提供的信息，对用户来说也是不易获得的，原因是这些信息过度分散于多个文件中，需要用户经过五六个步骤才能访问。

2.违反了为广告个性化处理提供法律依据的义务。

首先，用户的“同意”并未充分了解情况。比如 Google 对广告进行了稀释操作，打散在 Google 搜索、You tube、Google 主页、Google 地图、Playstore、Google 图片中，个人信息在多个文件中被过度传播（预计 20 个）。

其次，用户的“同意”既不是具体的也不是明确的。创建帐户后，用户可以通过单击“更多选项”按钮修改与帐户关联的某些选项，在“创建帐户”按钮上方访问。实际上，用户不仅必须点击“更多选项”按钮来访问配置，而且还预先勾选了广告个性化的显示。

但是，根据 GDPR 的规定，只有用户明确的肯定行动（例如勾选未预先勾选的方框），同意才是“明确的”。

最后，在创建帐户之前，要求用户勾选“ 我同意 Google 的服务条款 ” 框 和 “ 我同意如上所述处理我的信息，并在隐私政策中进一步说明”才能完成创建帐户的过程。

合规启示

1. 企业应当以简单明了、透明以及易获得的形式将 GDPR 第 13 条和第 14 条要求提供的信息提供给数据主体，特别注意相关信息不应过度分散，确保用户能够通过相对容易的操作访问其个人数据；

2. 对数据收集和处理的目的描述应当是明确而清晰的；

3.选择和适用恰当的合法性基础；

4.在获取用户的同意时，应当确保该同意是明确而具体的，即针对不同的处理行为获取相应的同意，禁止”一揽子“授权同意。

02 SERGIC 数据泄露事件

- **处罚金额**
  40 万欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/5/28

案件事实概述

SERGIC 公司专门从事房地产的推销、购买、销售、租赁和物业管理服务，拥有 486 名员工，2017 年营业额约为 4,300 万欧元。

CNIL 的处罚决定基于两个理由：缺乏基本的安全措施和违反存储限制原则。关于第一个问题，无需任何身份验证程序便可以在线访问租赁者上传的敏感个人数据，包括身份证、健康卡、税务通知单、家庭津贴发放单、离婚判决、账单报表等。尽管该漏洞自 2018 年 3 月以来就为公司所知，但直到 2018 年 9 月才最终得到解决。此外，该公司的文档存储时间超过了必要限制。

CNIL 在作出处罚决定时考虑了以下因素：违规行为的严重性、公司规模及其财务状况。

违规分析

1.无需身份验证程序便可在线访问租赁者上传的敏感文件，技术和组织措施不足，无法确保个人数据的安全性和机密性。

2. 数据留存及存储期限超过了处理目的所必要的限制。

合规启示

1. 采取相关技术和组织措施，确保个人数据的安全性和机密性，例如对访问数据的申请者进行身份验证；

2. 应对数据泄露事件时， 事前形成相对完善的数据泄露响应制度，采取防护措施，事中采取及时调查、主动上报、积极止损的方式，与监管机构保持良好密切的沟通，将影响控制在尽可能小的范围内；

3.遵守数据存储限制原则，以可识别数据主体身份形式存储的个人数据存储时间不能超过实现处理目的所必需的的时间。

03 ACTIVE ASSURANCES 数据泄露事件

- **处罚金额**
  18 万欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/7/25

案件事实概述

2018 年 6 月 1 日，CNIL 接到客户投诉称其无需事先的身份验证程序就可以访问该公司网站上其他用户的个人数据，包括驾驶执照副本、车辆登记证、银行对帐单和有关吊销驾照的信息。用户在设置帐户后会收到一封电子邮件，其中标识了用户名和密码，但未进行加密。该公司辩称，向 CNIL 举报的投诉人具有 IT 专业背景，没有相关技能的自然人无法识别出此安全缺陷。但 CNIL 对此并不认可。想要提高数据安全性和更改密码的客户被强制采用生日格式的密码。CNIL 对该公司密码管理提出了质疑，该公司辩称对密码复杂性的选择是出于方便客户以满足他们轻松访问其个人数据的愿望。

本案还有一个细节值得关注：2019 年 6 月 11 日，该公司提交了异议。但由于这些邮件是在 2019.5.29 法令第 40 条第 3 款规定的十五天期限届满后发送的，因此 CNIL 宣布不接受该异议。

违规分析

1.当访问数据的请求发送到服务器时，服务器必须首先验证请求者是否有权访问所请求的数据。在本案中，投诉人和检查团都可以自由地查阅公司注册客户的文件，而该公司没有采取任何限制措施来阻止访问；

2.客户帐户密码的保密强度较低。想要提高数据安全性和更改密码的客户被强制采用生日格式。此外，还通过电子邮件向公司客户发送密码，发送未加密的电子邮件可能会导致任何收听网络并了解其中包含的信息的人对其进行拦截。没有采取任何其他措施来验证人员身份，例如限制密码错误时的尝试次数。

合规启示

1.在客户注册个人账户时应充分提示其设置密级较高的密码以保护个人账户的安全，不能强制用户使用密度低的密码；

2.充分遵守 GDPR 第 32 条的规定，采取适当的技术和组织措施来保证所处理的个人数据的安全性和保密性；

3.在收到相关调查通知时，应密切关注当地法律的特殊规定，比如一些时限要求，以免丧失异议或抗辩权。

04 员工投诉某公司监控侵犯隐私事件

- **处罚金额**
  2 万欧元
- **处罚依据**
  Art. 5 (1) c) GDPR,
  Art. 12 GDPR,
  Art. 13 GDPR,
  Art. 32 GDPR
- **处罚时间**
  2019/6/13

案件事实概述

在 2013 年至 2017 年期间，CNIL 收到该公司几名员工的投诉，这些员工称某公司在他们的工作场所安装监控摄像头进行拍摄。CNIL 两次提醒该公司注意在工作场所安装视频监视设备时要遵守的规则，特别是禁止侵犯员工隐私，员工不应被连续拍摄，以及必须提供有关数据处理的合法依据。但该公司没有采取适当的措施，CNIL 于 2018 年 10 月进行了第二次检查，确认该公司在使用 CCTV 录制员工时仍然违反 GDPR。该公司也不要求员工在计算机上使用密码进行保护，并且所有员工使用唯一且共享的登录名和密码来访问企业电子邮件（该公用邮箱用于与客户沟通工作）。

在确定罚款金额时，CNIL 考虑了公司规模（9 名员工）和公司的财务状况（2017 年的净利润为负 885）。

违法分析

1.违反最小范围原则：公司出于确保人员和财产安全的目的安装视频监视设备，那么就应当充分考虑工作人员的数量、设备的安装位置、方向、操作周期等因素，特别应当禁止对员工进行持续和永久的监控；

2.违反了透明性原则。未按照 GDPR 第 12、13 条以简洁明了、透明、易获得的形式向员工提供应提供的信息，包括处理数据（视频监视设备录制）的目的和依据等；

3.缺乏技术和组织措施,无法保证个人数据的安全性和保密性。

合规启示

1.遵守数据最小范围原则，数据收集与处理应当是与目的相关的，且限于目的的最小必要范围。公司安装视频监视设备应当是出于确保人员和财产安全的目的，应避免对员工进行持续和永久的拍摄、禁止侵犯员工个人隐私；

2.收集和处理员工个人数据应当以简洁明了、透明、易获得的形式向员工提供应提供的信息，包括处理数据的目的和依据等；

3.采取适当的技术和组织措施以保证员工个人数据的保密性和安全性。

5.3 保加利亚

立法概况

- Electronic Communications Act
- Law Amending and Supplementing the Personal Data Protection Act
- Personal Data Protection Act

监管机构

Commission for personal data protection (CPDP, DPA)
网址: http://www.cpdp.bg/
E-mail : kzld@cpdp.bg
电话：+359 899 877 156
传真：+3592/91-53-525
DPO：Lyubomir Grancharov
Ralitsa Naumova - Assistant
DPO's e-mail: dpo@cpdp.bg

COMMISSION FOR PERSONAL DATA PROTECTION

01 国家税务局数据泄露事件

- **处罚金额**
  26 万欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/8/28

案件事实概述

黑客非法访问并分发了国家税务局持有的 600 万个数据主体的个人数据，包括联系信息、纳税申报信息和其他财务信息。数据主体包括在世的保加利亚及外国公民和已故者。

违法分析

缺乏保障信息安全的技术和组织措施。

合规启示

1. 重视并做定期的数据安全检查，在系统安全方面采取更多、有效的保护措施；

2. 应对数据泄露事件时， 事前形成相对完善的数据泄露响应制度，采取防护措施，事中采取及时调查、主动上报、积极止损的方式，与监管机构保持良好密切的沟通，并将数据泄露的事实告知数据主体，将影响控制在尽可能小的范围内。

02 DSK 银行数据泄露事件

- ❖ 处罚金额
  51.1 万欧元
- ❖ 处罚依据
  Art. 32 GDPR
- ❖ 处罚时间
  2019/8/28

■ 案件事实概述

DSK 银行发生数据泄露事件，该事件导致未经授权的第三方可以访问 23,000 多条信用记录，这些信用记录涉及超过 33,000 个银行客户，包括姓名、国籍、地址、身份证副本、生物识别数据及关联的第三方（包括配偶、子女和担保人）等个人数据。

■ 违规分析

缺乏保障信息安全的技术和组织措施。

■ 合规启示

1. 重视并做定期的数据安全检查，在系统安全方面采取更多、有效的保护措施。

2. 应对数据泄露事件时， 事先形成相对完善的数据泄露响应计划，采取防护措施，事中采取及时调查、主动上报、通知数据主体、积极止损的方式，与监管机构保持良好密切的沟通，将影响控制在尽可能小的范围内。

03 电信服务提供商未经授权处理个人数据

- ❖ 处罚金额
  2.71 万欧元
- ❖ 处罚依据
  Art. 5 (1) a) GDPR,
  Art. 6 GDPR
- ❖ 处罚时间
  2019/2/26

■ 案件事实概述

未经数据主体知悉和同意为其登记预付费业务。该电信服务提供商的雇员使用投诉者的个人数据注册登记了该公司的预付费服务，但数据主体并没有签署相关申请表。

■ 违规分析

1.处理个人数据没有合法性基础；

2.违反了数据处理的合法性原则。

■ 合规启示

数据处理应当合法，选择和适用恰当的合法性基础。

04 A.P. EOOD 非法处理个人数据

- 处罚金额
  5,100 欧元
- 处罚依据
  Art. 5 (1) a) GDPR,
  Art. 6 GDPR
- 处罚时间
  2019/3/26

案件事实概述

该行政管理机关非法处理个人数据。数据主体 D.D.的个人数据被用于制作一份就业合同，然而他当时正在监狱服刑。数据控制者在未经其知情和同意的情况下出于向 NRA 注册劳动合同的目的处理了他的个人数据。

违规分析

未经数据主体知情和同意处理其个人数据，没有合法性基础，违反了合法性原则。

合规启示

数据处理应当合法，选择和适用恰当的合法性基础。

05 某医疗中心非法处理个人数据

- 处罚金额
  510 欧元
- 处罚依据
  Art. 5 (1) a) GDPR,
  Art. 6 (1) GDPR,
  Art. 9 (1) and Art. 9 (2) GDPR
- 处罚时间
  2019/4/8

案件事实概述

因非法处理数据主体 G.B.的个人数据，对涉案的每个医疗中心处以 510 欧元的罚款。医疗中心 B 未经同意变更 G.B.的全科医生，使用软件自动生成一份全科医生变更登记表，提交给区域健康保险基金，然后提交给了另一个医疗中心，后者随后也非法处理了 G.B.的个人数据。

违规分析

1.数据处理没有合法性基础，违反数据处理的合法性原则。

2.违反关于特殊类型个人数据的处理规定，即禁止对健康数据、性生活或性取向等相关数据进行处理。

合规启示

数据处理应当合法，选择和适用恰当的合法性基础。特别是在涉及特殊类型个人数据处理时，应严格遵守 GDPR 及相关法律的规定。

06 某银行违反目的限制原则

- 处罚金额
  500 欧元
- 处罚依据
  Art. 5 (1) b) GDPR,
  Art. 6 GDPR
- 处罚时间
  2018/4/12

案件事实概述

该银行致电客户请求他的邻居偿还账单，该客户请求行使他的被遗忘权，在没有收到银行的任何答复后，他向 KZLD 投诉：银行处理客户个人数据的目的与履行客户信贷协议无关，即处理数据的目的与订立合同的目的不一致。

违规分析

违反目的限制原则，数据处理的目的与订立合同时的目的并不相关。

合规启示

1.遵守目的限制原则，基于具体、明确、合法的目的收集个人数据，且随后不得以与该目的相违背的方式进行处理。

2.如果出于不同的目的处理个人数据，该具体目的应当重新获得数据主体的同意。

07 某雇主未满足雇员行使访问权的要求

- 处罚金额
  500 欧元
- 处罚依据
  Art 5 (1) b) c) GDPR,
  Art. 12 GDPR,
  Art. 15 (1) GDPR,
  Art. 15 (1) a), b), c), g) GDPR,
  Art. 15 (3) GDPR
- 处罚时间
  2019/2/22

案件事实概述

一名雇员向其雇主发出了访问其个人数据的请求。该雇主没有及时、完整地答复该请求。

违规分析

在数据主体行权时，未能及时响应，且提供的信息不完整，违反了数据处理的合法、透明原则。

合规启示

对于数据主体行使访问权、更正权、删除权（被遗忘权）、限制处理权、数据可携权、拒绝权等基本权利时，数据控制者不得拖延，应及时、全面响应。

5.4 波 兰

Urząd Ochrony Danych Osobowych

■ 立法概况

- Processing Passenger Name Record Data Act
- Protection of Personal Data Act

■ 监管机构

The President of the Office for Personal Data Protection (UODO, DPA)
网址: https://www.uodo.gov.pl/
E-mail: kancelaria@uodo.gov.pl
电话：22 531 03 00
传真：22 531 03 01

01 西里西亚足球协会公开披露数据

- **处罚金额**
  12,950 欧元
- **处罚依据**
  Art. 6 GDPR
- **处罚时间**
  2019/4/25

■ 案件事实概述

2015 年 10 月至 2018 年 7 月，西里西亚足球协会公开披露了一些已获得裁判执照的裁判员的个人信息。披露的个人信息包括姓名、住址、PESEL 编号。披露行为没有任何合法性基础。该事件可能导致未经授权使用这些个人信息的潜在风险，例如冒充他人进行借贷或其他行为。

2018 年 8 月，该体育协会向监管机构报告了个人数据泄露事件，但是无法删除网上公开的数据，直到 2019 年 1 月才消除风险。因此受到监管部门的处罚决定。在决定处罚金额时，UODO 主席还考虑了其他因素，例如侵权行为持续时间、影响范围（涉及到 585 名裁判员）、严重性质、与监管部门的良好合作、非营利活动、被侵权人受到损害的证明等。

■ 违规分析

1.违反数据最小化原则。足球协会有义务在网站上保留授予裁判执照的相关记录，但应当限于处理目的所必要的范围。披露住址及 PESEL 编号超出了目的范围。

2.违反完整性和保密性原则。足球协会过度披露了裁判员的个人数据可能导致他人未经授权使用此类个人数据，存在严重的潜在风险。

3.2018 年 7 月至 2019 年 1 月未采取措施阻止进一步损害。在公开披露后，未采取措施阻止访问裁判员的个人数据以消除风险，导致不可控的数据共享带来进一步的损害。

4.未采取适当的技术和组织措施来确保处理数据的安全性。即使在通知受影响的数据主体的过程中，侵权行为仍在继续发生。足球协会委托第三方机构阻止非法访问，但未验证其行为和结果的有效性。

■ 合规启示

1.企业应当遵守数据最小化原则。处理个人数据应当与目的相称，不得公开披露超出目的范围外的数据类型。

2.数据控制者承担保证数据安全性及完整性的责任。发生数据泄露事件应当及时采取适当确保数据安全性的技术和组织措施，消除损害，防止进一步损失的发生。委托第三方处理泄露事件，应当验证委托方行为和结果的有效性。

02 Morele.net 数据泄露事件

- **处罚金额**
  644,780 欧元
- **处罚依据**
  Art. 5 (1) f) GDPR,
  Art. 32 GDPR
- **处罚时间**
  2019/9/10

案件事实概述

2018 年 10 月，波兰购物网站 Morele.net 遭受数据泄露。该事件导致约 220 万人的个人数据泄露。泄露的数据类型包括姓名、电话号码、电子邮件、收货地址，还有大约 35,000 人的分期贷款申请中涉及到的数据，包括个人 ID 号码（PESEL 号码）、身份证明文件的编号和序号、学历、注册地址、通信地址、收入来源、净收入金额、家庭生活费用、婚姻状况以及信用承诺或赡养义务的金额。

针对此次事件，UODO 对该购物网站做出 64 万欧元的处罚决定。

违规分析

1.该购物网站未采取适当的数据保护技术手段，无法有效监控典型在线行为有关的潜在风险，从而违反了第 5 条第 1 款（f）规定的保密原则。

2.数据泄露影响范围超过 220 万人，违规行为严重程度高，对受影响者产生极高的负面影响。

合规启示

1.企业采取适当的数据保护技术手段，提高数据安全性，有效监控业务场景中典型的潜在风险，对敏感或特殊类型个人数据进行加密等保障措施，及时识别风险并采取措施防范和阻止风险。

2.在发生数据泄露事件后，应当及时消除风险，阻止侵害行为进一步扩散，降低损害后果。

03 Bisnode 未履行充分性告知义务

- **处罚金额**
  219,538 欧元
- **处罚依据**
  Art. 14 GDPR
- **处罚时间**
  2019/3/26

案件事实概述

数字营销公司 Bisnode 从公开来源（尤其是从中央电子登记册和经济活动信息）获得数据主体数据，并出于商业目的处理该数据。涉及的数据主体超过 600 万人，但是只有 9 万多人被告知数据处理的情况，超过 1.2 万人不同意该公司处理其个人数据。该公司仅向留有邮箱地址的数据主体履行告知义务，对没有邮箱地址的数据主体以高额运营成本为由未履行告知义务，仅在其网站上提供了隐私政策条款。

针对此次事件，UODO 对该公司做出 219,538 欧元的处罚决定。

违规分析

1.未向部分数据主体履行告知义务。该公司收集的数据主体信息包括邮箱地址以及电话号码。因此可以通过邮箱地址或电话号码联系数据主体，履行告知义务。

2.具有侵权的故意。公司明知需要履行提供相关信息的义务以及直接告知相关人员的义务，但以部分数据主体没有提供电子邮箱地址为借口逃避责任。

3.配合程度低。在处以罚款时，未采取也不打算采取任何行动制止侵权行为。

合规启示

1.公开渠道获取数据主体个人数据用于商业目的的，应当向数据主体履行告知义务。应当采用一切可行的方式履行告知义务，只有在穷尽所有可能办法而无法实现时，才能采用公示告知的方式。

2.在与监管部门的沟通合作中应当积极配合，与监管机构保持良好密切的沟通，有助于将影响控制在尽可能小的范围内。

5.5 荷 兰

AUTORITEIT PERSOONSGEGEVENS

立法概况

- Implementation Act for the General Data Protection Regulation
- Telecommunications Act

监管机构

Dutch Data Protection Authority (DPA)
网址：https://autoriteitpersoonsgegevens.nl/
电话：(+31) - (0)70 - 888 85 00
传真：(+31) - (0)70 - 888 85 01

Authority for Consumers and Markets (NRA)
网址：https://www.acm.nl/en
电话：+31 70 7222 000
传真：+31 70 7222 355

01 Uber 数据泄露事件

UBER

- **处罚金额**
  60 万欧元
- **处罚依据**
  Art. 33 GDPR
- **处罚时间**
  2018/11/29

案件事实概述

2016 年，优步发生数据泄露事件，导致未经授权访问客户和驾驶员的个人数据。在发现违规行为后 72 个小时内优步没有向荷兰 DPA 和数据主体报告数据违规行为。此数据泄露事件已影响全球 5700 万 Uber 用户 ,并涉及 17.4 万荷兰公民。泄露的数据类型包括客户和司机的姓名，电子邮件地址以及电话号码。

针对该事件，荷兰数据监管部门对优步做出 60 万欧元的处罚决定。

违规分析

违反数据泄露报告义务，发生数据泄露事件后在 72 个小时内优步没有向荷兰 DPA 和数据主体报告数据违规行为。

合规启示

1. 企业应当在日常的经营活动中重视并定期开展合规性检查，在系统安全方面采取更多、有效的保护措施。

2. 应对数据泄露事件时， 事前形成相对完善的数据管理制度，采取防护措施，事中采取及时调查、在规定时间内主动报告监管部门和受影响的数据主体、采取积极止损的方式，与监管机构保持良好密切的沟通，有助于将影响控制在尽可能小的范围内。

02 Haga Hospital 未采取安全保密措施

- **处罚金额**
  46 万欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/6/18

案件事实概述

Haga 医院数十名职员不必要的查看一名有名的荷兰人的医疗记录。经调查发现，Haga 医院对于患者医疗记录没有采取合适的安全保密措施。

针对该事件，荷兰数据保护监管机构对该医院做出 46 万欧元的处罚决定。此外，为督促 Haga 医院改善患者记录的安全性，强加了一个整改处罚决定，如果 Haga 医院在 2019 年 10 月 2 日之前还未改善安全措施，该医院必须每两周支付 10 万欧元的罚款，总罚款数最高不超过 30 万欧元。Haga 医院表示将采取整改措施。

违规分析

1.未经数据控制者指示，有访问权限的职员不得处理患者的医疗记录，该医院职员未经指示访问行为违反 GDPR 第 32(4)条的规定。

2.医院没有采取足够的安全措施以确保患者医疗记录信息的安全。主要体现在两个方面：一是未定期检查有权访问医疗记录信息的主体，二是未采取多重验证访问身份的机制。

合规启示

1.企业应当采取措施确保任何对个人数据享有访问权限的雇员或其他授权主体非经指示不得处理这些数据。

2.企业应当在两方面采取充分的访问权限安全保障措施。一是定期检查访问记录，及时发现风险信号，对于未经授权查阅数据的行为采取措施。二是采取多重验证访问身份的机制，良好的安全性要求身份验证至少涉及两个因素。可以使用密码或密码结合员工通行证来确定访问身份。

5.6 葡萄牙

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

■ 立法概况

- Portuguese Data Protection Law (Law No. 58/2019 of August 8th)

■ 监管机构

Comissão Nacional de Protecção de Dados (CNPD, DPA)
网址：https://www.cnpd.pt/
电话：(+ 351) 21 392 84 00
传真：(+ 351) 21 397 68 32

01 Barreiro 医院过度访问患者档案

- **处罚金额**
  40 万欧元
- **处罚依据**
  Art. 5 (1) c) and f) GDPR
  Art. 32 GDPR
- **处罚时间**
  2018/7/17

■ 案件事实概述

2018 年 7 月 17 日，葡萄牙数据监管机构（CNPD）认定 Barreiro 医院违反 GDPR，并处以 40 万欧元的罚款。处罚理由如下：一是未将临床数据的访问权限分开，医院的医生都可以不受限制地访问所有患者档案；二是医院的个人资料管理系统存在缺陷，该医院只有 296 名医生，但在系统中具备访问功能的账户（医生）则多达 985 个。

违规分析

Barreiro 医院违反了 GDPR 第 5(1)f)条的“完整性和保密性”原则与 5(1)c)条的“数据最小化”原则。

合规启示

1.企业在进行个人数据的处理时，应通过技术组织措施，如设置有限的访问权限，保证数据的完整性和保密性，保障数据处理安全。

2.数据处理应当限于数据处理目的的最小范围。

5.7 西班牙

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

立法概况

- General Telecommunications Law
- Information Society Services Law
- Private Insurance and Reinsurance Intermediation Law
- Protection of Personal Data Law
- Retention of Data Law (Electronic Comms and Public Comms Networks)
- Royal Decree-Law 5/2018
- Royal Decree-Law 12/2018
- Royal Decree-Law 13/2012

监管机构

Agencia Española de Protección de Datos (DPA)
网址：https://www.aepd.es/
电话：901 100 099
912 663 517

01 LaLiga 未履行充分告知义务

- 处罚金额
  25 万欧元
- 处罚依据
  Art. 5 (1) a)　GDPR
  Art. 7 (3) GDPR
- 处罚时间
  unknown

案件事实概述

足球联盟（LaLiga）被罚款，原因是其提供的APP每分钟访问一次用户手机的麦克风。根据 AEPD 的意见，LaLiga 没有将这一事实充分告知用户。 此外，该应用程序不满足用户可以撤回同意的法律要求。

违规分析

未充分告知用户其提供的 APP 每分钟访问一次用户手机的麦克风，且剥夺了用户撤回同意的权利。

合规启示

1.相关 APP 的隐私设置中，在获取用户同意时，应当将相关处理事实充分告知用户；

2.采取简单易行的方式以供用户行使撤回同意的权利。

02 信贷公司未经授权处理个人数据

- 处罚金额
  6 万欧元
- 处罚依据
  Art. 5 (1) f GDPR
- 处罚时间
  Unknown

案件事实概述

该信贷公司将未还账单委托给收债公司。收债公司为索收欠款不仅向债务人发送电子邮件，还向债务人的工作公共邮箱发送催债通知，债务人的所有同事均可访问该公共邮箱，而债务人从未提供过该公共邮箱地址。

违规分析

催债信息不仅发送到已提供的个人邮箱，还发送到从未提供过的工作公共邮箱。

合规启示

1.委托第三方进行数据处理时，应当签订数据处理协议以规范数据处理者的处理行为合法、合规；

2.对处理者处理行为及责任不清楚，并不能成为免除控制者签署数据处理协议责任的抗辩理由。在该场景下进行的数据处理活动具有非常高的合规风险。

03 ENDESA 非法披露个人数据

- 处罚金额
  6 万欧元
- 处罚依据
  Art. 5 (1) f) GDPR
- 处罚时间
  Unknown

■ 案件事实概述

投诉人的银行账户被 ENDESA 收取一笔费用，该笔费用受益人是第三人，该第三人曾因刑事犯罪被下发两年期的限制令，该限制令禁止其接近投诉人、投诉人的住所及工作场所。ENDESA 没有按照投诉人的要求修改合同，而是错误地删除了她的个人数据，并将第三人的个人数据填入合同中。AEPD 认为，向第三方披露投诉人的个人数据严重违反了保密原则。

■ 违规分析

错误地删除个人数据，并将第三人的个人数据填入合同中，非法向第三方披露个人数据。

■ 合规启示

1.企业应当采用适当的技术组织措施保护数据免遭未经授权或非法的处理以及意外的丢失、销毁和破坏。

2.企业应保持其处理的数据适时地更新，并采取一切合理的措施确保错误数据被及时清除或更正。

04 AVON COSMETICS 非法处理个人数据

- 处罚金额
  6 万欧元
- 处罚依据
  Art. 6 GDPR
- 处罚时间
  2019/8/16

■ 案件事实概述

一位消费者称，雅芳化妆品公司非法处理其个人数据，未充分验证他的身份，导致他的数据被错误地记录在涉诉登记中，使其无法与银行建立合同关系。

■ 违规分析

非法处理个人数据，导致数据主体的个人数据被错误地记录在涉诉登记中。

■ 合规启示

企业处理客户个人数据应当充分验证其身份，避免错误的非法处理。

05 VODAFONE 未满足客户行使遗忘权的要求

- ❖ 处罚金额
  2.7 万欧元
- ❖ 处罚依据
  Art. 17 GDPR
- ❖ 处罚时间
  2019

■ 案件事实概述

尽管投诉人（曾是 Vodafone 的客户）曾在 2015 年要求 Vodafone 删除其个人数据，并且该请求已得到公司的确认，但自 2018 年起，他收到了 Vodafone 发送的 200 多条 SMS。沃达丰声明，发生这种情况是因为投诉人的手机号码被错误地用于测试，并错误地出现在其他客户档案中。由于该公司同意付款和承担责任，因此根据西班牙行政法将罚款减少至 27,000 欧元。

■ 违规分析

Vodafone 未充分响应客户删除其个人数据的权利。

■ 合规启示

企业应充分响应数据主体删除权的行使。同时应当适时更新保证数据的准确性，错误数据应当及时清除和更正。

06 VODAFONE 违反准确性原则

- ❖ 处罚金额
  5,000 欧元
- ❖ 处罚依据
  Art. 5 (1) d GDPR
- ❖ 处罚时间
  2018

■ 案件事实概述

西班牙电信局（SETSI）作出决定认定沃达丰应当向一个客户退还其错误收取的费用。沃达丰仅退还了相关费用，但没有将关于这个客户的错误账单信息删除，依旧将该错误数据报送给了偿付中心（BADEXCUG）。 AEPD 认定这种行为违反了准确性原则。

■ 违规分析

沃达丰将客户的错误账单数据报送给了偿付中心，违反了准确性原则。

■ 合规启示

企业应保持其处理的数据适时地更新，并采取一切合理的措施确保错误数据被及时清除或更正。

5.8 德 国

立法概况

- Criminal Code 1871
- Data Protection Adaptation and Implementation Act 2017
- Federal Data Protection Act 2017
- Federal Data Protection Act 1990 (No longer in force)
- Federal Office for Information Security Act 1990
- Freedom of Information Act 2005
- Identity Cards and Electronic Identifications Act 2009
- Social Code - Book X - Social and Administrative Procedures and Protection of Social Data 1980
- Telecommunications Act 2004
- Telemedia Act 2007

监管机构

The Federal Commissioner for Data Protection and Freedom of Information (BfDI，DPA)
网址: https://www.bfdi.bund.de/DE/Home/home_node.html
E-mail: poststelle@bfdi.bund.de
电话：+49 (0)228-997799-0
传真：+49 (0)228-997799-5550

The Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway(BNetzA，NRA)
网址：https://www.bundesnetzagentur.de/EN/Home/home_node.html
E-mail:info@bnetza.de
电话：+49 228 14-0
传真：+49 228 14-8872

01 Delivery Hero 未满足用户权利要求

- 处罚金额
  195,407 欧元
- 处罚依据
  Art. 15 GDPR,
  Art. 17 GDPR,
  Art. 21 GDPR
- 处罚时间
  2019/8

案件事实概述

有十名数据主体称已经有十年不曾使用过该公司的交付服务平台，但该公司仍然没有删除前客户的账号。此外，八位前客户抱怨该公司未经授权发送电子邮件广告。其中一位明确反对将其数据用于广告投放，但仍收到了 15 封电子邮件广告。有五名前客户抱怨，该公司没有向数据主体提供所需的信息，或者仅在柏林数据保护官员进行干预之后才提供数据。

针对此次事件，柏林数据保护局对该公司做出 19.5 万欧元的处罚决定。

违规分析

1.在前客户要求删除其个人数据时，没有履行删除义务，违反了 GDPR 第 17 条关于被遗忘权的规定。

2.前客户明确拒绝为广告营销目的处理其个人数据，该公司仍向其推送广告电子邮件，违反 GDPR 第 21 条关于拒绝权的规定。

3.该公司未在一个月内回应数据主体行使访问权的要求，违反了 GDPR 第 15 条关于访问权的规定。

合规启示

1.当数据主体要求删除其个人信息时，数据控制者应当立即履行删除义务。

2.为营销目的处理个人数据，应当征得数据主体同意。当数据主体明确拒绝为广告营销目的处理其个人数据时，数据控制者不得向其推送广告。

3.当数据主体行使访问权时，数据控制者应当在法律规定期限内（一个月内）回应数据主体的行权要求，特殊情况下可以延长至两个月。

02 某银行未经授权处理个人数据

- 处罚金额
  5 万欧元
- 处罚依据
  Art. 6 GDPR
- 处罚时间
  2019/3

案件事实概述

某银行未经授权使用所有前客户的个人数据——用于黑名单管理，拒绝为这些客户提供新帐户。该银行辩称，根据《德国银行法》其有义务对涉嫌洗钱的客户采取安全措施。柏林监管机构认为这是非法的。当局认为，这种做法将侵犯到没有涉嫌洗钱的客户的个人数据权利。

针对此次事件，柏林数据保护局对该银行做出 5 万欧元的处罚决定。

违规分析

未经授权处理前客户的个人信息，且没有其他合法性基础 ,违反 GDPR 第 6 条关于合法性基础的规定。

合规启示

企业收集、处理个人信息应当具有合法性基础。

03 某企业数据泄露事件

- 处罚金额
  2 万欧元
- 处罚依据
  Art. 33 (1) GDPR,
  Art. 34 (1) GDPR
  Art. 83 (4) a) GDPR
- 处罚时间
  2018

案件事实概述

发生数据泄露事件后，迟延上报监管部门，并且未通知数据主体。

针对此次事件，汉堡数据保护局做出 2 万欧元的处罚决定。

违规分析

发生数据泄露事件迟延上报监管部门，并且未通知数据主体。

合规启示

在发生个人数据泄露的情形时，数据控制者应当自发现之时起 72 小时内，报告监管机构，并向数据主体履行告知数据泄露的义务。

04 Knuddels 未加密用户个人数据

- **处罚金额**
  2 万欧元
- **处罚依据**
  Art. 32(1)(a) GDPR,
- **处罚时间**
  2018/11/21

案件事实概述

2018 年夏，Knuddels 公司被黑客攻击。该事件导致大约 33 万用户的登录密码和电子邮件地址被窃取并发布。经调查显示，该公司并没有加密其客户的密码及邮件信息，而是将其以纯文本形式存储。

数据泄露事件爆发后，Knuddels 公司立刻以广泛且透明的方式告知用户黑客攻击情况。并以一种“典范方式”向德国巴登符腾堡州数据保护委员会报告了该数据违规事件，披露其数据处理、公司结构、安全漏洞情况。

在审理过程中，公司实施了综合措施，以改善其 IT 安全架构，并将最新的技术应用于保障其用户数据的安全性。此外，公司承诺与巴登-符腾堡州数据保护局（LfDI）合作，实施额外措施，进一步提高其数据安全水平。

针对此次事件，LfDI 在计算罚款时，考虑到 Knuddels 公司在其指导方案和建议方面的高度配合及其合规的强烈意愿，最终按照较低标准定，仅仅罚款 2 万欧元。

违规分析

公司并没有加密其客户的密码及邮件信息，而是将其以纯文本形式存储，违反了 GDPR 第 32.1 条规定的确保个人数据处理安全的义务（“对个人数据进行假名和加密的义务”）。

合规启示

1. 建立流程以及时检测和报告数据泄露是至关重要的。

2. 在大规模数据泄露事件中，及时通知个人数据泄露情况可能会为接下来的监管调查提供有力证明。

3. 学习如何管理声誉影响。在 LfDI 声明中，LfDI 仅提到执法涉及位于巴登 - 符腾堡州的社交媒体提供商（尽管媒体很快确定了新闻稿背后的提供商）。从这一点来看，有一个积极的信息：通过与监管机构的合作，仍有可能被描述为“良好的企业公民”。

05 Kolibri Image 未签署数据处理协议

- **处罚金额**
  5,000 欧元
- **处罚依据**
  Art. 28 (3) GDPR,
- **处罚时间**
  2018/12/17

案件事实概述

Kolibri Image 已向 Hessen 数据保护局发送请求，询问如何与不想签署处理协议的服务提供商打交道。在没有更详细地回答 Kolibri Image 之后，案件被转发给当地负责的汉堡数据保护局。

2018 年 5 月，汉堡数据保护局（HHDSB）要求 Kolibri 公司与提供客户数据处理咨询的指定邮政服务供应商 Packlink 签署数据处理协议。针对此次事件，HHDSB 对该公司做出 5000 欧元的罚款。

Kolibri 公司指出该违规行为发生于 GDPR 生效前，且没有证据证明在 2018 年 5 月 24 日后还存在违规行为。该申诉理由被接纳。

2019 年 4 月 3 日，HHDSB 撤回处罚决定并终止处罚程序。

违规分析

根据 GDPR 第 28 (3) 条规定，数据处理者的处理行为应当受到合同或其他法律规定的法律行为的约束，该合同对数据处理者和控制者都有法律约束力，并确立处理行为的内容和期限、性质和目的、个人数据的类型和数据主体的种类以及数据控制者的权利和义务。公司指定第三方供应商处理客户数据，未签署数据处理协议，在不知道供应商数据处理的流程下，还将数据传送给处理者，违反 GDPR 第 28 (3) 条规定。

合规启示

1.个人数据由第三方处理时，必须签订数据处理协议，应当包括处理行为的内容和期限、性质和目的、个人数据的类型和数据主体的种类、保护数据而采取的技术和组织措施的细节以及数据控制者的权利和义务。

2.对处理者处理行为及责任不清楚，并不能成为免除控制者签署数据处理协议责任的抗辩理由。在该场景下进行的数据处理活动具有非常高的合规风险。

06 个人未经授权披露他人个人数据

- **处罚金额**
  2,000 欧元
- **处罚依据**
  Art. 5 GDPR
  Art. 6 GDPR
- **处罚时间**
  2019/2/5

案件事实概述

2018 年 7 月至 9 月期间，某名男子采用抄送方式向多人发送电子邮件，而非密送，导致每个人可以看到其他人的个人邮箱地址。2018 年 7 月中旬至 7 月末，该名男子被指控涉及 10 起侵权行为。据披露，在他的邮箱列表中 131~153 个个人的邮箱地址可以被识别到。

针对此次事件，萨克森 - 安哈尔特数据保护局对该名男子做出 2000 欧元的罚款决定。

违规分析

该名男子使用抄送方式向多人发送电子邮件，属于向第三方披露电子邮件地址的个人数据，属于个人数据的处理行为。处理个人数据应当具备合法性基础。而本案中该名男子未经数据主体同意，且不具备其他合法性基础，违反了 GDPR 关于合法性基础的规定。

合规启示

在范围内发送电子邮件的场景中，如果收件人彼此没有披露的合理性理由，企业应当采取密送方式保护每个收件人的个人邮箱地址不向其他第三人披露。向第三方披露个人信息，应当取得数据主体的同意或其他合法性基础。

07 警官非法处理个人数据

- **处罚金额**
  1,400 欧元
- **处罚依据**
  Art. 6 GDPR
- **处罚时间**
  2019/5/9

案件事实概述

2019 年 5 月，一名警官利用其公职身份通过联邦汽车运输管理局的中央交通信息系统（ZEVIS）查询有关他不熟悉的车主牌照信息，后利用此信息与联邦网络管理局进行 SARS 调查，询问受害人的个人数据以及存储在系统中的家庭及个人联系方式，在没有任何官方理由或当事人同意的情况下与受害人取得联系。

针对此次事件，巴登-符腾堡州数据保护局（LfDI）对该名警官做出 1400 欧元的罚款。

违规分析

警官出于私人目的，而非履行行政职责，因此该侵权行为归因于其个人，与公共部门无关，不适用《巴登-符腾堡州数据保护法》（LDSG）第 28 条规定（根据该规定，GDPR 的制裁不适用于公共机构）。

合规启示

1.本案是德国第一起处罚公权力机构雇员的案例。

2.收集、处理个人信息应当具有合法性基础。未经授权或不具有其他合法性基础，不得收集、处理个人数据。

5.9 希 腊

立法概况

- A bill of law (published on February 20, 2018, but has not been enacted yet.)
- Law 4624/2019 - Law on Personal Data Protection, Implementing Measures of Regulation (EU) 2016/679

监管机构

Hellenic Data Protection Authority (HDPA, DPA)
网址：https://www.dpa.gr/
E-mail：contact@dpa.gr
电话：+30-210 6475600
传真：+30-210 6475628

Hellenic Authority for Communication Security and Privacy (ADAE, NRA)
网址：http://www.adae.gr/
E-mail：info@adae.gr
电话：+30-210 6387600
+30-210 6387601
传真：+30-210 6387666

01 PWC 处理员工个人数据违反透明原则

- **处罚金额**
  15 万欧元
- **处罚依据**
  Art. 5 (1) a), b) and c) GDPR,
  Art. 5 (2) GDPR, Art. 6 (1) GDPR,
  Art. 13 (1) c) GDPR,
  Art.14 (1) c) GDPR
- **处罚时间**
  2019/7/30

案件事实概述

使用不恰当的法律依据处理其员工个人数据——选择同意作为其数据处理的合法性基础。雇佣关系下数据主体的同意不能认定为基于自由意志（自愿）作出的，因当事方的权力并不平等。以不公平且不透明的方式处理其员工的个人信息——使员工错误地认为公司基于GDPR第6条第（1）款（a）项，实际是基于员工从未被告知的其他法律依据进行处理的。违反可问责性原则——PWC BS 负有证明其数据处理行为符合 GDPR 的义务，但其无法提供 HDPA 要求的说明其合法性基础的内部文件；此外，公司将合规义务转移给员工：要求他们签署声明：声称知晓其个人数据被公司记录和处理，并认同数据处理行为与雇佣关系和工作的开展相关，并且是恰当的。

违规分析

1.错误地使用同意作为其处理员工个人数据的合法性基础，违反了合法性原则；

2.违反了透明性原则，因此违反了 GDPR 第 13（1）（c）和 14（1）（c）条规定的提供信息的义务；

3.违反问责制原则，未能向 HDPA 提供证明其已对处理员工个人数据的法律基础进行了事先评估。

合规启示

1.合法、公平、透明原则要求仅在其他合法性基础不适用的情况下才将同意作为合法性基础处理员工个人数据；

2.明确告知员工收集其个人数据的目的和用途以及处理员工个人数据的法律依据等 GDPR 要求提供的信息；

3.对处理行为进行记录与存档，是员工数据保护合规的运行结果与证据。

5.10 罗马尼亚

立法概况

- Law No. 129 of 2018 on the Processing of Personal Data
- Law No. 190 of 2018 on Measures to Implement GDPR

监管机构

National Supervisory Authority for Personal Data Processing (DPA)
网址：https://www.dataprotection.ro/
E-mail: dpo@dataprotection.ro or anspdcp@dataprotection.ro
电话： +40.318.059.211
传真： +40.318.059.602

01 UNICREDIT 银行数据泄露事件

- **处罚金额**
  13 万欧元
- **处罚依据**
  Art. 5 (1) c) GDPR
  Art. 25(1) GDPR
- **处罚时间**
  2019/6/27

案件事实概述

由于未能实施适当的技术组织措施保障数据安全，UNICREDIT 银行在 2018 年 5 月 25 日至 2018 年 12 月 10 日期间，内外部交易中 337,042 个数据主体的身份信息和地址在网上被泄露。

违法分析

未能实施适当的技术组织措施保障数据安全。

合规启示

企业应当采取适当的技术组织措施保证个人数据安全，免遭数据泄露。

02 WORLD TRADE CENTER 数据泄露事件

- **处罚金额**
  15,056 欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/7/2

案件事实概述

World Trade Center 发生客户个人数据泄露事件。用于检查客户早餐情况的纸质清单中包含该酒店 46 位客户的个人数据，这些数据被外部未经授权的人员拍摄并线上发布。该数据控制者已受到制裁，因为它没有采取措施确保数据安全。

违规分析

未采取适当的技术组织措施保障数据安全，导致包含该酒店的 46 位客户的个人数据被公司外部的未经授权的人员拍照，导致数据泄露。

合规启示

企业应当保证数据处理在适当的技术组织措施下，免遭未经授权或非法的处理。

03 LEGAL COMPANY & TAX HUB SRL 数据泄露事件

- **处罚金额**
  3,000 欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/7/5

案件事实概述

没有采取足够的技术和组织措施保障数据安全。某些文件在 2018 年 12 月 10 日至 2019 年 2 月 1 日期间可通过两个链接公开访问。在 avocatoo.ro 网站上进行交易的人员的个人数据（姓名，姓氏，邮寄地址，电子邮件，电话，职业，进行的交易的详细信息）遭受了未经授权的披露和访问。监管机构在 2018 年 10 月 12 日发出通知后实施了制裁。

违规分析

未采取足够的技术和组织措施保障数据安全，导致个人数据遭到未经授权的披露和访问。

合规启示

企业应当采取适当的技术组织措施保证个人数据免遭未经授权的访问或非法处理。

04 UTTIS 未履行充分告知义务

- **处罚金额**
  2,500 欧元
- **处罚依据**
  Art. 5 (1) c) GDPR
  Art. 6 GDPR
  Art. 12 GDPR
  Art. 13 GDPR
- **处罚时间**
  2019/7

案件事实概述

该数据控制者无法证明有关数据主体充分了解其个人数据(图像)被视频监控系统处理和使用，该视频监控系统自 2016 年就开始运作。

此外 ,该数据控制者向公司通告人展示员工 2018 年认证 ISCIR 培训报告时披露了员工的 CNP，但无法证明其公开 CNP 的合法性基础，违反了 GDPR 第 6 条。

违法分析

1.未履行充分性告知义务；

2.不能证明数据主体了解其个人数据被处理；

3.处理员工 CNP 没有合法性基础。

合规启示

1.视频监控需要设置明确的隐私政策或标识，履行充分告知义务；

2.数据处理要有合法性基础 ,严禁非法处理员工个人数据。

5.11 匈牙利

立法概况

- Amendment of Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information

监管机构

National Authority for Data Protection and Freedom of Information (DPA)
网址：http://www.naih.hu/
E-mail：ugyfelszolgalat@naih.hu
电话：+36 (1) 391-1400
传真：+36 (1) 391-1410

National Media and Infocommunications Authority (NMHH, NRA)
网址：http://english.nmhh.hu/
E-mail：info@nmhh.hu
电话：(06 1) 457 7100
传真：(06 1) 356 5520

01 SZIGET 音乐节和 VOLT 音乐节的组织者收集过度个人数据

- **处罚金额**
  92,146 欧元
- **处罚依据**
  Art. 5 (1) b) GDPR
  Art. 6 GDPR
  Art. 13 GDPR
- **处罚时间**
  2019/5/23

案件事实概述

活动组织者为实现安保目的，收集和存储了数据主体的以下信息：国籍，姓名，性别，证件类型，证件编号，有效期，出生日期，图像和声音数据。以上个人数据由卡夫特公司“记录、存储和管理”。但 NAIH 认为组织者可以通过不涉及个人数据的筛查措施，例如金属探测器或安全筛查等措施实现安保目的。

违规分析

1.使用不恰当的法律依据。数据控制者错误地适用活动参与者的知情同意作为合法性基础，并且其获得的同意也不是有效的，因为如果活动参与者拒绝提供相关信息，他将被拒绝入场。但事实上其出于维护活动参与者的生命和人身安全这一基本人权、避免其遭受大规模恐怖事件的目的。经过 NAIH 进行利益平衡测试，认定应当适用的合法性基础是 GDPR 第 6 条第（1）款（f)项：为追求合法利益目；

2.未遵守目的限制原则。组织者可以通过不涉及个人数据的筛查措施，例如金属探测器或安全筛查等措施实现安保目的。

合规启示

1.数据处理应选择和适用恰当的合法性基础，并对自己的处理行为符合 GDPR 规定承担责任并予以证明；

2.遵守目的限制原则，基于具体、明确、合法的目的收集个人数据，且随后不得以与该目的相违背的方式进行处理；

3.遵守数据处理的透明性原则。

02 匈牙利政党数据泄露事件

- **处罚金额**
  34,375 欧元
- **处罚依据**
  Art. 33 (1) GDPR
  Art. 33 (5) GDPR
  Art. 34 (1) GDPR
- **处罚时间**
  2019/4/5

案件事实概述

该政党数据库遭到黑客入侵，该黑客访问并披露了包含 6000 多人的数据，其中包含特殊类型个人数据。该政党组织网页系统安全性差，很容易受到攻击。黑客发布攻击指令后，即使是 IT 知识水平较低的人也可以从数据库中访问信息。

且该政党未在 72 小时内将数据泄露通知 NAIH 和相关数据主体 ,并且未根据 GDPR 第 33 条第（5）款记录和保存违规情况。

根据法律规定，罚款的依据是该党年度营业额的 4%和来年预期营业额的 2.65%。

违规分析

1.技术和组织措施不足，无法确保个人数据的安全性和机密性；

2.违反数据泄露报告义务；

3.违反数据泄露记录的有关规定；

4.违反向数据主体告知数据泄露的义务。

合规启示

1. 采取相关技术和组织措施，确保个人数据的安全性和机密性，例如对访问数据的申请者进行身份验证；

2. 应对数据泄露事件时， 事前形成相对完善的数据泄露响应制度，采取防护措施，事中采取及时调查、主动上报、积极止损的方式，与监管机构保持良好密切的沟通，将影响控制在尽可能小的范围内；

3.遵守数据泄露事件有关记录的规定，记录有关泄露事实、影响及采取的补救措施。

03 匿名主体数据泄露事件

- **处罚金额**
  15,150 欧元
- **处罚依据**
  Art. 33 GDPR
- **处罚时间**
  2019

■ 案件事实概述

该数据控制者丢失了包含个人数据的闪存驱动器，且未在 72 小时内履行其数据泄露报告义务。

■ 违规分析

违反数据泄露报告义务。

■ 合规启示

1. 采取相关技术和组织措施，确保个人数据的安全性和机密性，例如对访问数据的申请者进行身份验证。

2. 应对数据泄露事件时， 事前形成相对完善的数据泄露响应制度，采取防护措施，事中采取及时调查、主动上报、积极止损的方式，与监管机构保持良好密切的沟通，将影响控制在尽可能小的范围内。

3.遵守数据存储限制原则，以可识别数据主体身份形式存储的个人数据存储时间不能超过实现处理目的所必需的的时间。

04 匿名主体未满足数据主体权利实现要求

- **处罚金额**
  3,200 欧元
- **处罚依据**
  Art. 12 (4) GDPR
  Art. 13 GDPR
  Art. 15 GDPR,
  Art. 18 (1) c) GDPR
- **处罚时间**
  2018/12/18

■ 案件事实概述

数据控制者未向数据主体提供 CCTV 记录，未保留记录以供数据主体进一步访问及使用，未告知数据主体其有向监管机构投诉的权利。

■ 违规分析

1.未响应数据主体行权请求；
2.未履行 GDPR 关于数据处理记录的规定；
3.违反数据处理的透明性原则。

■ 合规启示

1.对于数据主体行使访问权、更正权、清除权（被遗忘权）、限制处理权、持续控制权、拒绝权等基本权利时，数据控制者不得拖延，应及时将所请求的信息提供给数据主体；

2.注重数据的存储、归档和管理，避免意外或非法销毁，丢失，更改，未经授权的披露或访问。

05 市长办公室非法处理个人数据

- 处罚金额
  3,200 欧元
- 处罚依据
  Art. 5 (1) a) GDPR
  Art. 6 GDPR
- 处罚时间
  2019/2/28

■ 案件事实概述

因非法披露举报人的个人信息而对凯奇凯梅特市市长办公室处以罚款。某组织的一名雇员向凯奇凯梅特市市长办公室提出了对其雇主的举报投诉。雇主要求提供详细信息，该市长办公室透露了投诉人的名字。雇主随后解雇了举报人。

■ 违规分析

数据处理违反遵守合法性原则。

■ 合规启示

严禁非法数据处理，包括非法收集、记录、存储、改编、传播或披露等。

06 某金融机构拒绝删除客户个人数据

- 处罚金额
  3,200 欧元
- 处罚依据
  Art. 5 (1) b) and c) GDPR
  Art. 6 (4) GDRP
  Art. 13 (3) GDPR
  Art. 17 (1) GDPR
- 处罚时间
  2019/3/4

■ 案件事实概述

NAIH 对一家未具名的金融机构处以罚款，理由是该公司非法拒绝客户要求删除其电话号码的请求，理由是保留该客户的电话号码对客户进行债务索偿符合公司的合法利益。NAIH 在其决定中强调，客户的电话号码对于催收债务不是必需的，因为债权人也可以通过邮寄方式与债务人进行通信。因此，保留债务人的电话号码违反了数据最小化和目的限制的原则。根据法律规定，罚款的评估依据是公司年度净收入的 0.025%。

■ 违规分析

1.未满足数据主体行使被遗忘权的要求；

2.违反数据最小化和目的限制原则。

■ 合规启示

1.对于数据主体行使访问权、更正权、清除权（被遗忘权）、限制处理权、持续控制权、拒绝权等基本权利时，数据控制者不得拖延，应及时将所请求的信息提供给数据主体；

2.遵守数据最小范围原则 ,数据收集与处理应当是与目的相关的，且限于目的的最小必要范围。

07 某金融机构违反数据处理基本原则

- **处罚金额**
  1,560 欧元
- **处罚依据**
  Art. 5 (1) b) and c) GDPR
- **处罚时间**
  2019/2/20

案件事实概述

收债员出于识别目的收集数据主体的出生地、母亲姓氏等详细信息；某个数据主体要求提供有关数据并删除该数据，而收债员拒绝了删除请求，并说明无法识别该数据主体，并辩称根据《会计法》和内部政策，其有法律义务保留备份。但由于上述法律规定及内部政策没有正确告知数据主体（其应当以透明和详细的方式将备份副本告知数据主体），也没有向数据主体提供以下信息：存储的个人数据种类、保留期限、副本的可能使用方式以及删除日期。NAIH 认为收债员违反了数据处理的最小化原则和透明性原则。罚款占其年度利润的0.0025%。

违规分析

1.违反数据处理的最小化原则；

2.违反数据处理的透明性原则。

合规启示

1.遵守数据最小范围原则 ,数据收集与处理应当是与目的相关的，且限于目的的最小必要范围；

2.公司内部有关数据处理的所有政策对客户都应透明。

08 某银行处理个人数据违反准确性原则

- **处罚金额**
  1,560 欧元
- **处罚依据**
  Art. 5 (1) d) GDPR
- **处罚时间**
  2019/2/8

案件事实概述

客户在开设银行账户时提供了错误的电话号码，银行错误地将该名客户的信用卡债务信息通过 SMS 消息发送到另一个人的电话号码。客户通知银行电话号码错误，但银行未响应数据主体清除错误数据的要求，而是继续向错误的电话号码发送 SMS 消息。罚款占银行年利润的0.0016%。

违规分析

违反数据处理的准确性原则,且对数据主体的行权（更正权）不及时响应。

合规启示

1.遵守数据处理的准确性原则，若有必要应保持适时更新，采取一切合理性措施确保与数据处理目的相悖的错误数据被及时清除或更正；

2.对于数据主体行使访问权、更正权、清除权（被遗忘权）、限制处理权、持续控制权、拒绝权等基本权利时，数据控制者不得拖延，应及时将所请求的信息提供给数据主体。

5.12 捷 克

立法概况

- Act On Personal Data Processing Act 110/2019 (in Czech)
- On Personal Data Processing Amending Certain Related Laws 111/2019 (in Czech)

监管机构

Office for Personal Data Protection (OPDP, DPA)
网址: https://www.uoou.cz/
电话：+420 234 665 800 (GDPR infoline)
+420 234 665 111 (Phone)
+420 234 665 555
+420 234 665 444

01 某网络购物商城数据泄露事件

- **处罚金额**
  5.8 万欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2018

案件事实概述

2014 年 12 月 31 日至 2017 年 7 月 23 日，一家网络购物商城发生数据泄露事件，并于 2017 年 8 月 25 日上报。该网络购物商城的客户用户账号数据库被窃取，导致 766421 个电子记录泄露，其中包括 735956 个独特的电子邮件地址。泄露的数据类型包括客户的电子邮箱、加密密码、姓名、电话号码。

针对此次事件，捷克数据保护监管机构对该网络购物商城做出 5.8 万欧元的处罚决定。

违规分析

该网络购物商城未采取保障信息安全的适当的技术和组织措施，导致发生数据泄露事件，影响范围大，性质较为严重。

合规启示

企业应当采取适当的安全保障技术及组织措施，事前采用日志系统等安全保障措施记录数据处理行为，及时预警风险信息。重视日常的系统安全维护。发生数据泄露事件后，应及时采取应对措施，积极消除风险，阻止损害进一步扩大。

02法国巴黎银行个人理财公司违反数据处理基本原则

- **处罚金额**
  9,704 欧元
- **处罚依据**
  Art. 5 (1) c) and e) GDPR
- **处罚时间**
  2019/3/21

案件事实概述

法国巴黎银行个人理财公司向客户提供贷款业务。客户可以选择向该公司申请贷款，或向该公司的零售商申请分期贷款业务。当客户选择后者时，零售商会处理其个人数据，其他情况下，零售商不会保留客户个人数据。此外，信息技术提供商也存在处理个人数据的行为。法国巴黎银行与零售商和服务提供商都签署了数据处理协议。采用电子形式签署协议时，法国巴黎银行在履行法定义务及获得用户明示同意的基础上，收集用户的生物特征签名数据。此外在合同履行完毕后，法国巴黎公司继续存储与客户的通话录音长达 10 年。

针对该事件，捷克数据保护监管部门对该公司做出 9704 欧元的处罚决定。

违规分析

1.违反数据最小范围原则。生物签名并非处理目的所必须的条件，客户的身份识别可以采用其他方式足以得到验证，也可以采取签署书面协议，同样具有约束力；

2.违反存储限制原则。法国巴黎银行处理与经常账户申请有关的个人数据的处理时间超过了处理目的所需的期限，且超过了销毁数据所指定的期限。

合规启示

1.收集个人数据应当遵守最小范围原则，收集的数据应当是充足的、与处理目的相关的并且限于数据处理目的最小必要范围；

2.存储个人数据应当遵循存储限制原则，存储时间不能长于实现个人数据处理目的所必须的时间，不能超出销毁数据所指定的期限。

03 某银行未经授权处理客户个人数据

- **处罚金额**
  3,105 欧元
- **处罚依据**
  Art. 5 (1) a) and b) GDPR
  Art. 32 (1) GDPR
- **处罚时间**
  2019/5/13

案件事实概述

自 2012 年以来，投诉人一直作为公司银行帐户的法定代表人，授权银行收集和处理他的个人数据，包括姓名、姓氏、社会保险号、出生日期、性别、出生地、国籍、身份证号码。2018 年 10 月 10 日 ,投诉人收到了未经授权办理的账户借记通知信息。据银行称，该卡于 2017 年 6 月 21 日由投诉人在 PragueHolešovice 分支机构开设了活期账户，但未发现合同文件。该账户开设未经授权，当事人接受索赔后，该账户于 2018 年 11 月 20 日关闭。

针对该事件，捷克数据保护监管部门对该公司做出 3105 欧元的处罚决定。

违规分析

1.该银行未经授权使用客户个人数据为客户开设银行账号，违反 GDPR 关于合法性基础的规定，以及与数据处理最初的目的不一致，违反了目的限制原则；

2.该银行未采取保障信息安全的适当的技术和组织措施 ,导致客户个人数据被非法使用。

合规启示

1.使用个人信息应当具有合法性基础，未经授权且没有其他合法性基础不得处理个人信息。基于具体、明确、合法的目的收集个人数据，且随后不得以与最初目的相违背的方式处理数据；

2.企业应当采取适当的安全保障技术及组织措施保障客户个人数据安全，防止未经授权或非法的处理以及意外的丢失、销毁或破坏。

04 INTER-IVCO 未经授权公开披露个人数据

- **处罚金额**
  3,105 欧元
- **处罚依据**
  Art. 6 GDPR
- **处罚时间**
  2018

案件事实概述

INTER-IVCO 运营一个网站，名为 www.rejstrikdluhu.cz，可以用来查询债务人的信息。有用户投诉，受到匿名邮件告知其负担债务的通知。据调查，INTER-IVCO 未对网站访问设定任何限制规则，每个人都可以在支付一定费用并同意通用条款的情况下，访问未履行债务的信息。据悉，通过这个网站已经有 431 名申请人获得总数 779 项信息 ,涉及的数据类型包括姓名、地址、债务信息、虚拟的债权人。此类信息的披露未获得数据主体的授权同意。

针对此次事件，捷克数据保护监管机构对该公司做出 3480 欧元的处罚决定。

违规分析

INTER-IVCO 作为数据控制者，公开披露数据主体的个人数据未获得数据主体同意且不具备其他合法性基础，违反了 GDPR 关于合法性基础的规定。

合规启示

作为数据控制者，收集、使用、公开披露数据主体个人数据应当获得数据主体同意或有其他合法性基础。

05 汽车租赁公司未履行充分告知义务

- **处罚金额**
  1,165 欧元
- **处罚依据**
  Art. 5 (1) a) GDPR
  Art. 6 GDPR
- **处罚时间**
  2019/2/4

案件事实概述

至少在 2018 年 5 月 24 日至 10 月 23 日期间，汽车租赁公司未告知数据主体有关通过放置在车辆中的 GSP 定位器收集、处理其个人数据的相关信息。

针对此次事件，捷克数据保护监管机构对该汽车租赁公司做出 1165 欧元的处罚决定。

违规分析

汽车租赁公司未告知数据主体有关通过放置在车辆中的 GSP 定位器收集、处理其个人数据的信息、个人数据控制者的身份和联系方式、处理个人数据的目的以及处理的法律依据等信息，违反了 GDPR 第 5 条第 1 款（a）项规定的处理个人数据应遵守合法、公平和透明原则。

合规启示

1.数据控制者收集、处理个人数据应遵守合法、公平和透明原则，告知数据主体关于数据收集类型、处理目的、合法性基础、个人数据控制者的身份和联系方式、存储期限（在无法确定具体时间的情况下，提供确定存储期限的标准）、安全保障、数据主体权利等信息；

2.数据控制者处理个人数据应当获得数据主体同意，或具有其他合法性基础。

06 信贷经纪公司违反数据完整性与保密性要求

- **处罚金额**
  1,165 欧元
- **处罚依据**
  Art. 5(1) f) GDPR
  Art. 32 GDPR
- **处罚时间**
  2019/2/4

案件事实概述

信贷经纪公司作为信贷调解中客户个人数据的管理者，将已失效的合同存放在公寓楼普通车库的纸箱中至少 14 天，直到 2018 年 8 月 23 日被发现，导致大约 300 名客户的个人数据被泄露。合同中包括的个人数据类型有名称、姓氏、社会保险号、身份证号码、家庭住址、电话号码和信用信息等。2018 年 8 月 28 日捷克数据保护监管部门收到该公司发送的个人数据泄露通知。

针对此次事件，捷克数据保护监管机构对该公司做出 1165 欧元的处罚决定。

违规分析

信贷经济公司将失效合同放置于公共区域，且并未采取任何安全销毁措施，违反了 GDPR 第 5 条第 1 款（f）以及第 32 条规定，即违反数据完整性与保密性的要求。

合规启示

1.数据控制者处理、存储个人数据应确保充分保护个人数据，通过采取适当的技术或组织措施保护其免受未经授权或非法处理以及意外丢失、破坏或损坏；

2.对于失效合同或其他不必要的个人数据应及时采取安全销毁等措施删除、销毁数据。

07 食品经销商缺乏数据处理合法性基础

- **处罚金额**
  1,160 欧元
- **处罚依据**
  Art. 5(1) a) GDPR
  Art. 32 GDPR
- **处罚时间**
  2018

案件事实概述

NatureMed Pharmaceuticals 是一家食品经销商，使用分发优惠券、邮件推送、电话营销等方式推销产品。客户信息来源于原客户以及另外购买或租赁的其他来源数据库。该公司的营销行为受到大量用户投诉，一方面新客户质疑该公司获得其个人数据的渠道，另一方面原客户称已拒绝并撤回处理个人信息的同意后还收到商家的联系。

针对此次事件，捷克数据保护监管机构对该公司做出 1160 欧元的处罚决定。

违规分析

1.在购买或租赁其他来源数据库时，缺乏数据处理的合法性基础。未检查及确认数据库中的数据主体是否做出同意授权及其同意的范围，是否同意数据转移；

2.在使用原客户个人信息时，数据主体已明确表示拒绝或撤回同意，该公司仍与其联系推销产品，违反对数据主体权利的保障；

3.违反履行告知义务。该公司对数据主体的告知信息并不充分，主要问题在于缺乏对数据处理目的及过程及合法性基础的说明。

合规启示

1.直接收集、使用个人数据时，应确保取得数据主体同意。当数据主体行使拒绝权或撤回同意时，应当响应数据主体的权利，不得再处理相关数据；

2.间接收集、使用个人数据时，应核查并确认数据提供方取得数据主体授权的情况及范围；

3.应当恰当履行对数据主体的告知义务，尤其是需要说明收集、处理个人数据的目的、处理过程及其合法性基础。

08 某公司未满足数据主体行使访问权的 fangwenquan 要求

- **处罚金额**
  776 欧元
- **处罚依据**
  Art. 15 GDPR
- **处罚时间**
  2019/2/26

案件事实概述

2018 年 11 月期间，投诉人多次电话联系某公司要求其删除他的个人数据。该公司收到删除请求后与投诉人取得了联系。2018 年 11 月 30 日，投诉人通过电子邮件要求该公司提供有关其个人数据处理的信息。截至 2019 年 2 月 18 日至 19 日，投诉人未收到该方提供的有关处理个人数据的任何信息。

针对此次事件，捷克数据保护监管机构对该公司做出 776 欧元的处罚决定。

违规分析

根据 GDPR 第 15 条第 1 款，数据主体有权从数据控制者处获得有关是否处理与他有关的个人数据的确认，数据控制者有义务在 GDPR 第 12 条规定的期限内（即在一个月内）对行使该权利的数据主体的要求做出回应，在特殊情况下可以将其延长两个月。该协会未在一个月内回应数据主体行使访问权的要求，违反了 GDPR 第 15 条规定。

合规启示

当数据主体行使访问权时，数据控制者应当在法律规定期限内（一个月内）回应数据主体的行权要求，特殊情况下可以延长两个月。

09 Christ Car Wash 数据泄露事件

- **处罚金额**
  695 欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2018

案件事实概述

ChCW的62名员工档案发生数据泄露事件，28 名员工收到匿名人发送的电子邮件，其中附带其人事资料的文件副本。据调查，ChCW 在雇员的人事档案中收集了很多文件副本信息，涉及的数据类型包括员工身份证、出生证明、健康卡、健康保险登记卡、违法犯罪记录核查、银行卡及银行账户，此外还收录了部门员工子女出生证明及员工照片的资料。发生数据泄露事件后，ChCW 未采取任何措施阻止个人信息及敏感信息的泄露。据调查，ChCW 公司处理人事信息时未采取日志功能，因此无法查验处理人事信息的访问人及访问原因，没有相应的访问记录。

针对此次事件，捷克数据保护监管机构对 ChCW 做出 695 欧元的处罚决定。

违规分析

1.违反目的限制原则和最小范围原则。收集、处理个人信息必须符合处理目的，ChCW 在没有明确处理目的的情况下收集用户的个人信息，违反目的限制原则和最小范围原则；

2.未采取保障信息安全的适当的技术和组织措施。ChCW 公司处理人事信息时未采取日志功能，因此无法查验处理人事信息的行为人主体及原因，没有出于人事管理目的访问个人数据的电子记录，未采取适当的安全保障措施，且在数据泄露事件发生后，未采取有效措施阻止数据泄露进一步扩散。

合规启示

1.收集、处理个人信息应当遵守目的限制原则和最小范围原则。收集、处理的个人信息应当是充分的、相关的，并且与处理目的相关；

2.企业应当采取适当的安全保障技术及组织措施，事前采用日志系统等安全保障措施记录数据处理行为，及时预警风险信息。发生数据泄露事件后，应及时采取应对措施，积极消除风险，阻止损害进一步扩大。

10 某公司数据泄露事件

- **处罚金额**
  582 欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/2/28

案件事实概述

在 2018 年 4 月 21 日至 2018 年 5 月 25 日期间，该公司在互联网地址上发布了游戏玩家的个人数据，大约持续 30 分钟，导致玩家名称、游戏帐户密码、游戏帐户 ID、电子邮件地址和 IP 地址未经授权公开披露。

针对此次事件，捷克数据保护监管机构对该公司做出 582 欧元的处罚决定。

违规分析

该公司未采取保障信息安全的适当的技术和组织措施，导致不适当公开个人数据，发生数据泄露事件。

合规启示

企业应当采取适当的安全保障技术及组织措施，事前采用日志系统等安全保障措施记录数据处理行为，及时预警风险信息。重视日常的系统安全维护。发生数据泄露事件后，应及时采取应对措施，积极消除风险，阻止损害进一步扩大。

11 某学校未满足数据主体权利实现要求

- **处罚金额**
  388 欧元
- **处罚依据**
  Art. 6 GDPR
  Art. 17 GDPR
- **处罚时间**
  2019/1/10

案件事实概述

2018 年 8 月 16 日一名某学校的前员工向捷克数据保护监管机构投诉。她在 2017 年在学校担任讲师，后来担任公司经理。离职后，2018 年 7 月上旬她发现学校 Facebook 网站上有她的照片和姓名，要求学校负责人从互联网上删除她的所有照片。但是学校没有删除。

针对此次事件，捷克数据保护监管机构对该学校做出 388 欧元的处罚决定。

违规分析

1.学校作为数据控制者，未经雇员同意将其姓名和照片个人信息发布在公开网络上，违反了 GDPR 关于合法性基础的规定；

2.在前雇员要求删除其个人信息时，没有履行删除义务，违反了 GDPR 第 17 条关于被遗忘权的规定。

合规启示

1.数据控制者处理个人数据应当获得数据主体同意，或具有其他合法性基础。未经同意或不具有其他合法性基础，不得收集、使用、披露个人数据；

2.在数据主体撤回同意或当个人数据处理已不必要情况下，数据主体提出删除其个人数据的请求时，数据控制者有必要立即采取删除措施，清除与数据主体相关的个人数据。

12 某协会未满足数据主体权利实现要求

- **处罚金额**
  388 欧元
- **处罚依据**
  Art. 15 GDPR
- **处罚时间**
  2018/10/25

案件事实概述

2018 年 6 月 19 日投诉人向某协会提出要求，访问其个人数据的处理信息，并要求删除其个人数据。2018 年 8 月 21 日，投诉人的个人信息已从该协会网站上删除。截止到 2018 年 10 月 19 日，投诉人未获得关于其个人数据处理情况的任何通知。

针对此次事件，捷克数据保护监管机构对该协会做出 388 欧元的处罚决定。

违规分析

根据 GDPR 第 15 条第 1 款，数据主体有权从数据控制者处获得有关是否处理与他有关的个人数据的确认，数据控制者有义务在 GDPR 第 12 条规定的期限内（即在一个月内）对行使该权利的数据主体的要求做出回应，在特殊情况下可以将其延长两个月。该协会未在一个月内回应数据主体行使访问权的要求，违反了 GDPR 第 15 条规定。

合规启示

当数据主体行使访问权时，数据控制者应当在法律规定期限内（一个月内）回应数据主体的行权要求，特殊情况下可以延长两个月。

13 某公司未满足数据主体权利实现要求

- **处罚金额**
  194 欧元
- **处罚依据**
  Art. 16 GDPR
- **处罚时间**
  2019/5/6

案件事实概述

申诉人与受诉公司2017年9月1日至2017年12月31日存在劳动雇佣关系。2018年2月15日申诉人从公司领取收入证明材料后发现，有3张收据在收据金额上有所不同且填写的地址和社会保险号等信息错误，要求公司对错误信息进行修改。2018年3月22日，根据公司要求，申诉人通过电子邮件反馈了雇员卡信息，其中包含姓名、头衔、永久地址、出生日期、出生地、国籍、性别、地位、身份证号码、健康状况、电子邮件地址、电话号码、纳税申报单、工作类型和受雇时间等个人信息发送给相关会计人员。截至2019年1月28日，申诉人仍然尚未收到信息更正的通知。

针对此次事件，捷克数据保护监管机构对该公司做出194欧元的处罚决定。

违规分析

该公司未响应数据主体关于更正错误信息的要求，违反了GDPR关于更正权的规定。

合规启示

当数据主体要求更正错误个人数据时，数据控制者应当及时响应数据主体行权要求，立即更正与其有关的错误数据。

5.13 意大利

立法概况

- GDPR Harmonization Law
- European Act 2017

监管机构

Italian Data Protection Authority (DPA)
网址：http://www.garanteprivacy.it/
E-mail: garante@gpdp.it; urp@gpdp.it
电话：+39-06-6967 71
传真：+39-06-6967 73785

01 意大利某政党数据泄露事件

- **处罚金额**
  5 万欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/4/17

案件事实概述

意大利政党 Movimento 5 Stelle 附属的许多网站都通过名为 Rousseau 的平台运行，Rousseau 为数据处理者。

Rousseau 平台在 2017 年夏遭受数据泄露，意大利数据保护机构（Garante）要求实施多项安全措施，此外还要求其更新隐私政策以提供更高的信息透明度。在隐私政策更新完成的同时，Garante 对 Rousseau 平台上缺少某些 GDPR 规定的安全保障措施表示关注。

值得一提的是，该违规行为始于 2018 年 5 月或更早，但 Garante 是根据 GDPR 的规定进行罚款的，罚款依据是 Rousseau 平台未采取 GDPR 所要求的安全保障措施。

另外，有意思的是罚款不是针对数据控制者 Movimento 5 Stelle，而是针对数据处理者 Rousseau。

违法分析

数据处理者缺乏保障数据安全的技术和组织措施。

合规启示

作为平台型的数据处理者，也应关注并保证数据处理安全，采取适当的技术组织措施，谨防数据泄露。

5.14 奥地利

立法概况

- Banking Act
- Data Protection Act (DSG) (amendments incorporating GDPR)
- E-Commerce Act, 2002
- Health Telematics Act, 2012

监管机构

Data Protection Authority (DSB, DPA)
网址：https://www.dsb.gv.at/
E-mail：dsb@dsb.gv.at
电话：+43 1 52 152-0

Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR, NRA)
网址：https://www.rtr.at/en/rtr/RTRGmbH
E-mail：mailto: rtr@rtr.at
电话: +43 1 58058-0
传真: +43 1 58058-9191

01 医疗公司未履行充分告知义务

- **处罚金额**
  5 万欧元
- **处罚依据**
  Art. 13 GDPR
  Art. 37GDPR
- **处罚时间**
  2018/8

案件事实概述

某医疗公司不遵守收集信息告知义务，且没有任命 DPO。

针对该事件，奥地利数据保护局对该医疗公司做出 5 万欧元的处罚决定。

违规分析

该医疗公司作为数据控制者的核心业务涉及大规模特殊类型个人数据（健康数据等）的处理，根据 GDPR 第 37 条，应当指定一名数据保护专员。该医疗公司未任命 DPO，违反了 GDPR 相关规定。

合规启示

当企业作为数据控制者或处理者核心业务由数据处理组成或涉及到GDPR规定的特殊类型个人数据或与犯罪记录、违法行为有关数据组成时，应当任命 DPO。

02 足球教练非法收集个人数据

- **处罚金额**
  1.1 万欧元
- **处罚依据**
  Art. 6 GDPR
- **处罚时间**
  2019/7

案件事实概述

Mostviertel 俱乐部的一名足球教练在一个淋浴间里放置智能手机对女运动员进行偷拍。

针对该事件，奥地利数据保护局对该教练作出 1.1 万欧元的处罚决定。

违规分析

未经授权拍摄属于侵犯个人隐私的行为，违反 GDPR 规定，甚至有可能承担刑事责任。

合规启示

收集、处理个人数据应当具有合法性基础。

03 博彩商店未履行充分告知义务

- 处罚金额
  4,800 欧元
- 处罚依据
  Art.13 GDPR
- 处罚时间
  2018/12/9

案件事实概述

2018 年 9 月，一家博彩商店在其店面前安装了一台闭路电视摄像机，同时对其店面前的人行道进行监控拍摄，未提示监控范围。

针对该事件，奥地利数据保护局对该商店做出 4800 欧元的处罚决定。

违规分析

该商店未将监控区域明确标识出来，大范围的公共空间设施被不正当记录。个人以这种方式监控公共区域，是不被允许的。

合规启示

1.企业在工作环境中应当在监控区域设置提醒，标识监控范围，履行告知义务；

2.收集个人数据应当遵守最小范围原则，收集的数据应当是充足的、与处理目的相关的并且限于数据处理目的的最小必要范围。

04 私人家中安装监控过度收集个人数据

- 处罚金额
  2,200 欧元
- 处罚依据
  Art. 5 (1) a) and c) GDPR
  Art. 6 (1) GDPR
  Art. 13 GDPR
- 处罚时间
  2018/12/20

案件事实概述

某人在家中的门窗区域安装了至少两个摄像头。视频监控覆盖范围超出了监控住宅区的一般用途，即：停车场，人行道，庭院，花园和住宅区的通道；视频监控范围覆盖了相邻物业的花园区域。

违规分析

1.违反必要性原则。视频监控收集的信息范围超过监控目的的必要限度，过度收集数据；

2.未经授权收集他人个人数据。视频监控记录了房屋的走廊和进出周围公寓的居民，未经同意记录他人图像数据，侵犯他人高度个人化的生活领域；

3.未履行告知义务。未明确标识监控区域范围。

合规启示

1.收集个人数据应当遵守必要性原则 ,收集的数据类型和范围应当与处理目的相一致；

2.收集个人数据应当具有合法性基础。未经授权且没有其他合法性基础不得收集个人数据；

3.采用摄像监控方式的 ,应当在监控区域设置提醒，标识监控范围，履行告知义务。

5.15 瑞 典

立法概况

- EU GDPR Supplementary Provisions Act
- EU GDPR Supplementary Provisions Ordinance
- Electronic Communications Law
- Marketing Act

监管机构

Swedish Data Protection Authority (DPA)
网址：https://www.datainspektionen.se/
E-mail：datainspektionen@datainspektionen.se
电话：08-657 61 00

Swedish Post and Telecom Authority (PTS, NRA)
网址：https://www.pts.se/en-gb/
E-mail：pts@pts.se
电话：+46 8 678 55 00
传真：+46 8 678 55 05

01 学校使用人脸识别技术缺乏合法性基础

- **处罚金额**
  18,630 欧元
- **处罚依据**
  Art. 5 (1) c) GDPR
  Art. 9 GDPR
  Art. 35 GDPR
  Art. 36 GDPR
- **处罚时间**
  2019/8/20

案件事实概述

一个名为 Anderstorps 的高中学校使用人脸识别技术来记录学生的上课考勤。学校董事会正在考虑将此技术作为标准程序来实施，其目的是进一步简化操作并自动进行课程注册。该学校董事会在一个实验项目中使用面部识别技术对学生的面部信息进行了登记。该实验项目持续了三周，涉及到 22 名学生。学生们的面部生物识别数据及全名被相机以照片的形式捕获，这些信息被存储在没有连接互联网的本地计算机中。学校在收集学生的生物识别数据之前征得了监护人的明确同意。但是，学校的这项行为并没有进行相关的风险评估，也没有事先与瑞典数据保护机构进行协商。

违规分析

1.违反目的限制和最小范围原则。为满足上课出勤统计的目的，学校可以以侵入性较小的方式实现，面部识别软件的使用与目的不成比例；

2.GDPR 原则上禁止以识别自然人身份为目的处理生物特征数据，除非符合例外情形。然而由于学校与学生之间关系的不平等性，监护人同意不能视为自愿 ,因此该同意存在瑕疵，不能作为合法性基础；

3.学校对人脸识别的风险评估缺乏该数据收集、处理行为对数据主体权利和自由存在的风险的评估，也缺乏与其处理目的相关的比例方面的评估和说明。

合规启示

1.对于人脸识别等生物特征数据的使用应持谨慎态度。根据数据最小化原则，处理的个人数据应该是充分的、相关的，并且与处理它们的目的相关，而不能过于全面的收集、处理数据。只有在用其他方法无法以令人满意的方式实现处理目的时，才可以考虑使用此类敏感数据，否则将存在较大的合规风险；

2.同意作为合法性基础存在较大风险。首先，同意作为合法性基础之一，只有在其他合法性基础不适用的情况下才得以适用。其次，同意需要符合自愿、自由要求。双方地位不平等将导致同意因欠缺自愿要素而失去效力。尤其在雇佣关系中，需谨慎应用同意；

3.新技术投入使用时，应当重视风险评估合规工作。形式主义的风险评估无法被监管部门认可，风险评估必须包含对处理目的必要性及相称性的评估和说明、对数据主体权利和自由存在的风险的评估等内容。

5.16 比利时

立法概况

- Data Protection Act

监管机构

Data Protection Authority (DPA)
网址：https://www.gegevensbeschermingsautoriteit.be/
E-mail: contact@apd-gba.be
电话： +32 (0)2 274 48 00
传真： +32 (0)2 274 48 35
Belgian Institute for Postal services and Telecommunications (NRA)
网址：https://www.ibpt.be/en
E-mail：info@bipt.be
电话: 02 226 88 88
传真: 02 226 88 77

01 某店主过度收集客户个人数据

- **处罚金额**
  1 万欧元
- **处罚依据**
  Art. 5 (1) c) GDPR
- **处罚时间**
  2019/9/19

案件事实概述

某店主使用用户的电子身份证（eID）为用户创建会员卡。

违法分析

违反数据最小化原则。收集、处理个人数据应当满足限于处理目的所必要的范围。使用身份证信息创建会员卡超出了目的范围。

合规启示

企业应当遵守数据最小化原则。收集、使用个人数据应当与目的相称，不得收集、使用超出目的范围外的数据类型。

02 某市长非法处理个人数据

- **处罚金额**
  2,000 欧元
- **处罚依据**
  Art. 5 (1) b) GDPR
  Art. 6 GDPR
- **处罚时间**
  2019/5/28

案件事实概述

有一位投诉人向比利时数据保护局提出了对比利时某市长的投诉，认为市长滥用投诉人的个人邮箱向投诉人发送了竞选选举（拉票）信息。问题是，市长之所以会知道投诉人的个人邮箱，是由于投诉人之前曾委托一名建筑师向市长就一房地产交易事项进行了咨询沟通，这位建筑师在其发送的邮件中附上了投诉人的电子邮件地址。于是，市长在该市政选举的前一天，使用了投诉人的电子邮件地址，以“答复”的形式向投诉人发送了竞选（广告）信息。

违规分析

1.比利时数据保护局认为 GDPR 适用于任何控制者，当然也适用于市长等公共权力拥有人；

2.比利时某市长使用数据主体个人电子邮件地址并发送竞选信息的行为，已经超出个人数据主体当时提交个人邮件地址的目的，违反了 GDRP 中目的限制原则，市长获得的电子邮件地址必须收集用于特定目的，不得以与这些目的不相容的方式进一步处理。

合规启示

处理个人信息应当遵守目的限制原则，不得以与该目的相违背的方式处理个人数据。

5.17 挪 威

■ 立法概况

- Electronic Communications Act
- Personal Data Act
- Personal Data Regulations

■ 监管机构

The Norwegian Data Protection Authority (DPA)
网址: https://www.datatilsynet.no/
E-mail: postkasse@datatilsynet.no.
电话：+47 22 39 69 00

01 奥斯陆市教育局数据泄露事件

- **处罚金额**
  20.3 万欧元
- **处罚依据**
  Art. 32 GDPR
- **处罚时间**
  2019/4/29

■ 案件事实概述

奥斯陆市教育局（UDE）开发了一款新应用“ Skolemelding ”（即学校信息），用于使父母和老师更轻松地交流孩子们在学校的日常生活。该应用启动前未经过适当的测试，存在重大安全漏洞，从而暴露了 63,000 名儿童个人信息和通讯记录。

针对该事件，挪威数据保护监管机构对该教育办公室做出 20.3 万欧元的处罚决定。

02 卑尔根市的市政用户计算机系统安全问题

- **处罚金额**
  17 万欧元
- **处罚依据**
  Art. 5 (1) f) GDPR
  Art. 32 GDPR
- **处罚时间**
  2019/3

违规分析

该教育办公室开发的该应用程序存在重大安全漏洞 ,未在应用程序投入使用前进行测试，也未采取足够的安全措施以确保儿童个人信息和通讯记录的安全。

合规启示

1.在开发移动应用程序时，应当采取安全保护措施，重视产品的安全性和保密性。在投入使用前，应当进行充分测试，防止重大安全漏洞。

2.企业应当采取适当的安全措施以保护用户的个人数据。适当的安全措施包括但不限于评估个人数据是否以受保护的形式存储，是否通过安全连接对数据共享进行加密以及应用程序是否应用了受信任的证书等。

案件事实概述

卑尔根市的市政用户计算机系统未对其管理的一所市政小学的小学生及该学校雇员的个人数据采取安全保密措施，导致这些数据处于不受保护和公开的状态。在公共存储区中发现了一个包含 3.5 万名学生和员工登录凭证的文件。任何登录学校信息网站的人都可以访问到该学校小学生及雇员的个人信息。公开的数据类型包括用户名、密码、出生日期、地址、学校隶属关系和学校成绩的信息。

针对该事件，挪威数据保护监管机构对该市做出 17 万欧元的处罚决定。

违规分析

1.该市政用户计算机系统未采取适当的数据保护技术手段。登录系统的安全性非常差，未经授权的人可以在学习平台和学校的管理系统中访问用户名和密码。

2.未对儿童提供特殊保护。GDPR 中将儿童定义为特别脆弱的群体，应给予特殊保护。但该市并没有提供更高的保护力度。

合规启示

1.企业采取适当的数据保护技术手段，提高数据保护安全性，有效监控业务场景中典型的潜在风险，对敏感或特殊类型个人数据进行加密等保障措施，及时识别风险并采取措施防范和阻止风险。

2.对于儿童应当给予特殊保护，对儿童个人信息提供更高的保护力度，例如采取加密、严格管控访问权限等方式。

5.18 丹 麦

DATATILSYNET

■ 立法概况

- Danish Data Protection Act(became enforceable on May 25, 2018,the Danish Data Protection Act does not apply to Greenland and the Faroe Islands.)

■ 监管机构

Danish Data Protection Agency
(Datatilsynet, DPA)
网址：https://www.datatilsynet.dk/
电话：+45 33 19 32 00

Danish Business Authority (NRA)
网址：https://danishbusinessauthority.dk/
E-mail：erst@erst.dk
电话：+45 35 29 10 00

IDdesign a|s

01 IDdesign A / S 违反数据存储限制原则

- **处罚金额**
  200,850 欧元
- **处罚依据**
  Art. 5 (1) e) and (2) GDPR
- **处罚时间**
  2019/6/3

■ 案件事实概述

Datatilsynet 发现 IDdesign A / S 处理大约 385,000 名客户个人数据超出了初始处理目的所需的范围。

此外，该公司在各种 IT 系统中存储了客户发票信息及人员招聘信息，但没有在存储期限结束后删除相关数据。并且，对于其他已删除的数据，IDdesign A / S 也没有对删除个人数据的过程进行记录和存档。

请注意：由于丹麦法律没有像 GDPR 那样规定行政罚款（除非是简单的案件并且被告同意），因此罚款将由法院判处。

02 Taxa 4x35 违反数据存储限制原则

- **处罚金额**
  16 万欧元
- **处罚依据**
  Art. 5(1) e) GDPR
- **处罚时间**
  2019

案件事实概述

丹麦《市场营销法》第 10 条规定了客户就收到时事通讯给予同意的两年有效期，两年后应删除相关电话号码。并且，如果客户在系统中删除其个人资料，则有关该人的其他信息应在 6 个月内删除。用于客户订购和结算税款的个人数据由于不再需要识别客户，Taxa 4x35 应在两年后将其匿名化或删除，但 Datatilsynet 在对 Taxa 4x35 进行监督访问时发现，Taxa 4x35 只删除了客户的姓名，依然留存着客户的电话号码、乘车记录（约 8,873,333 次出租车行程）。因此，有关客户税收的信息（包括收款及收货地址）仍可以通过电话号码识别到特定自然人。且根据 Taxa 4x35 隐私政策，电话号码仅在五年后才会删除，这直接违反了存储限制原则。

违规分析

未严格遵守数据存储限制原则、最小范围原则、责任原则及丹麦关于数据留存期限的具体规定。

合规启示

1.严格遵守存储限制原则，个人数据的存储方式不能使识别数据主体的时间长于处理个人数据所需的时间。这意味着，当不再需要个人数据时，通常必须将其删除或匿名化；

2.根据责任原则，数据控制者必须记录并对数据处理记录进行存档；

3.遵守数据最小范围原则，数据收集与处理应当是与目的相关的，且限于目的的最小必要范围；

4.注意丹麦、爱沙尼亚有关部门法关于数据留存期限的具体规定。

请注意：由于丹麦法律没有像 GDPR 那样规定行政罚款（除非是简单的案件并且被告同意），因此罚款将由法院判处。

违规分析

未严格遵守数据存储限制原则及丹麦关于数据留存期限的具体规定。

合规启示

1.严格遵守存储限制原则，个人数据的存储方式不能使识别数据主体的时间长于处理个人数据所需的时间。这意味着，当不再需要个人数据时，通常必须将其删除或匿名化.；

2.注意丹麦、爱沙尼亚有关部门法关于数据留存期限的具体规定。

5.19 立陶宛

立法概况

- The Law on Legal Protection of Personal Data
  (Data Protection Law,came into force since July 16, 2018)

监管机构

State Data Protection Inspectorate (VDAI, DPA)
网址：https://www.ada.lt/
E-mail: ada@ada.lt
电话：(8 5) 271 2804, 279 1445
传真：(8 5) 261 9494

01 UAB MisterTango 数据泄露事件

- **处罚金额**
  6.15 万欧元
- **处罚依据**
  Art. 5 GDPR
  Art. 32 GDPR
  Art. 33 GDPR
- **处罚时间**
  2019/5/16

案件事实概述

在一次检查中，VDAI 发现 UAB MisterTango 处理的数据超出了实现数据处理目的所必需的范围。此外，由于技术和组织措施不足，2018 年 7 月 9 日至 10 日，支付数据可在网上公开获得，导致来自不同国家的 12 家银行的 9,000 笔付款受到了影响。UAB MisterTango 未按规定上报数据泄露情况。

违法分析

1.没有足够的技术和组织措施来确保个人数据安全，未履行数据泄露报告义务；

2.UAB MisterTango 处理的个人数据超出了付款人发起付款所必需的数量和范围，违反了最小范围原则。

合规启示

1. 企业应当采取相关技术和组织措施，确保个人数据的安全性；

2. 应对数据泄露事件时，事前形成相对完善的数据泄露响应制度，采取防护措施，事中采取及时调查、主动上报、积极止损的方式，与监管机构保持良好密切的沟通，并将数据泄露的事实告知数据主体，将影响控制在尽可能小的范围内；

3.遵守最小范围原则，数据限于数据处理目的的最小必要范围。

5.20 塞浦路斯

■ 立法概况

- The Law 125(I)/2018
- The Protection of Physical Persons Against the Processing of Personal Data and Free Movement of such Data

■ 监管机构

Office for Personal Data Protection (DPA)

网址：
http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument
E-mail: commissioner@dataprotection.gov.cy
电话：+357 22818456
传真：+357 22304565

Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR, NRA)
网址：http://www.ocecpr.org.cy/nqcontent.cfm?a_id=1
E-mail：Info@ocecpr.org.cy
电话：+357 22693000
传真：+357 22693070

01 新闻媒体非法披露个人数据

- 处罚金额
  1 万欧元
- 处罚依据
  Art. 6 GDPR
- 处罚时间
  2019

案件事实概述

该报纸以纸质和电子形式报道了一起非法拘留案件时泄露了所涉两名警员的姓名和照片，以及第三名警员的照片。CDPC 认为，仅通过提及其名字的首字母和/或其面部模糊和/或远距离拍摄的照片即可实现新闻报道这一目标，并且无法识别特定自然人，而且采取这些措施不会给报道中的案件性质带来任何变化。

在作出处罚决定时，Cyprian Data Protection Commissione 考虑了欧盟法院关于表达自由与需要特殊处理的隐私权之间的平衡。

违规分析

非法披露警员的姓名和照片。

合规启示

数据处理应当合法，当进行履行涉及公共利益的职责所必要的数据处理时，应符合相关国家的具体规定，并对处理行为设立更为精细的具体要求和其他措施来确保数据处理的合法与公平。

02 某医院未满足数据主体权利实现要求

- 处罚金额
  5,000 欧元
- 处罚依据
  Art. 15 GDPR
- 处罚时间
  2019

案件事实概述

一名患者向 CDPC 投诉，医院无法满足其访问自己医疗档案的要求，因为该医院无法识别和定位到患者的医疗档案。

违规分析

没有充分实现数据主体的访问权。

合规启示

1.对于数据主体行使访问权、更正权、删除权（被遗忘权）、限制处理权、数据可携权、拒绝权等权利时，数据控制者不得拖延，应及时、全面响应；

2.注重数据的存储、归档和管理，避免意外或非法销毁，丢失，更改，未经授权的披露或访问。

5.21 拉脱维亚

立法概况

- The Personal Data Processing Law(came into force on July 5, 2018)

监管机构

Data State Inspectorate(DSI, DPA)
网址：http://www.dvi.gov.lv/
E-mail: info@dvi.gov.lv
电话：67 22 31 31
传真：67 22 35 56

01 某商家未满足数据主体权利实现要求

- **处罚金额**
  7,000 欧元
- **处罚依据**
  Art. 17 GDPR
- **处罚时间**
  2019/8/26

案件事实概述

某在线商家提供服务过程中侵犯了用户的“被遗忘权”。数据主体多次要求删除其个人数据，尤其是手机号码，然而，商家未响应该请求并继续通过短信将广告消息发送给该手机号码。

违法分析

没有充分实现数据主体的被遗忘权。

合规启示

对于数据主体行使访问权、更正权、删除权（被遗忘权）、限制处理权、数据可携权、拒绝权等权利时，数据控制者不得拖延，应及时、全面响应。

5.22 马耳他

立法概况

- Data Protection Act 2018 (Act) (Chapter 586 of the Laws of Malta)

监管机构

Office of the Information and Data Protection Commissioner (IDPC, DPA)
网址：https://idpc.org.mt/en/Pages/Home.aspx
E-mail: idpc.info@idpc.org.mt
电话：(+356) 2328 7100

01 土地管理局数据泄露事件

- **处罚金额**
  5,000 欧元
- **处罚依据**
  Art. 5 GDPR
  Art. 32 GDPR
- **处罚时间**
  2019/2/18

案件事实概述

由于土地管理局网站上缺乏适当的安全措施，通过简单的 Google 搜索，公众就可以轻松访问超过 10GB 的个人数据。泄漏的大多数数据包含高度敏感的信息以及个人与管理局本身之间的往来信息。在马耳他，数据保护监管局可对公共机构或机关每次违规处以最高 25,000 欧元的行政罚款，并可对违法行为持续的每一天另处每日 25 欧元的罚款。对于处罚决定，土地管理局选择不上诉。

违法分析

网站系统缺乏适当的安全措施，通过简单的 Google 搜索，公众就可以轻松访问超过 10GB 的个人数据。

合规启示

企业应当采用适当的技术和组织措施保护数据安全，确保处理的个人数据免遭未经授权的访问或非法的处理以及意外的丢失、销毁和破坏。

6 案例索引

缩略语释义	
GDPR	《通用数据保护条例》（General Data Protection Regulation），欧盟个人数据保护法，2016 年 4 月 27 日通过，经过两年过渡期，于 2018 年 5 月 25 日正式生效，取代《数据保护指令（95/46/EC）》。
ePR	《欧盟电子隐私条例》(EU ePrivacy Regulation)，2017 年 1 月 10 日由欧洲委员会提议，尚未通过。该条例将取代目前已生效的《电子隐私指令》(EU ePrivacy Directive)，旨在规制电子通信服务并保护与用户终端设备相关的信息。
EEA	欧洲经济区(European Economic Area)，包括欧盟 28 国、冰岛、挪威和列支敦士登。
EDPB	欧洲数据保护委员会(European Data Protection Board)，指欧盟层面的数据保护监管，取代 WP29，由各成员国国家监管机构负责人和欧洲数据保护监管机构负责人或其代表组成，推动 GDPR 在各成员国的一致适用和促进各国国家监管机构之间的合作。
WP29	第 29 条工作组(The Article 29 Working Party)，指依据欧盟《数据保护指令(95/46/EC)》第 29 条设立的数据保护工作组，GDPR 生效后被 EDPB 所取代。
SA	国家监管机构(Supervisory Authorities)，指欧盟各成员国数据保护监管机构，同 DPA。
DPA	国家监管机构(Data Protection Authorities)，指欧盟各成员国数据保护监管机构，同 SA。
DPO	数据保护官(Data Protection Officer)，指监督组织机构内部个人数据处理的自然人。
DPIA	数据保护影响评估(Data Protection Impact Assessment)，指用于描述数据处理过程、评估其必要性和合比例性、协助管理对自然人权利和自由带来的风险并决定处理措施的方法。

7 结 语

中兴通讯数据保护合规部是集企业合规治理和行业法律研究于一体的专业化团队，主要研究方向包括全球数据保护立法态势跟踪及案例解读、数据保护专题性及国别性研究、国内外网络安全法律解读、法律法规与企业合规政策转化，在严谨、扎实的研究基础上打造了业内领先的数据保护合规体系。

数据法盟是国内知名的聚焦法务、合规、IT、律师及教授的高端数据发平台，关注数据隐私和数据安全的非盈利性学术组织，始终致力于整合法律、技术及媒体的专业数据法生态体、打造相互赋能及塑造职业品牌的数据法共同体。

《GDPR 执法案例精选白皮书》由中兴通讯数据保护合规部与数据法盟联合编制。白皮书致力于以第一视角审视欧洲数据保护监管脉搏，呈现 GDPR 执法案例全景图，对欧洲数据保护立法概况和执法案例进行一站式、综合性解读，有助社会公众、业内人士、政府官员对 GDPR 的切身感知和简明理解，强化数据保护专业领域内智力和信息互动，促进经验观点的倾听吸纳、合规治理的优化转化，推动中国企业数据保护合规工作进程。

中兴通讯数据保护合规部　　数据法盟

（2018~2019）