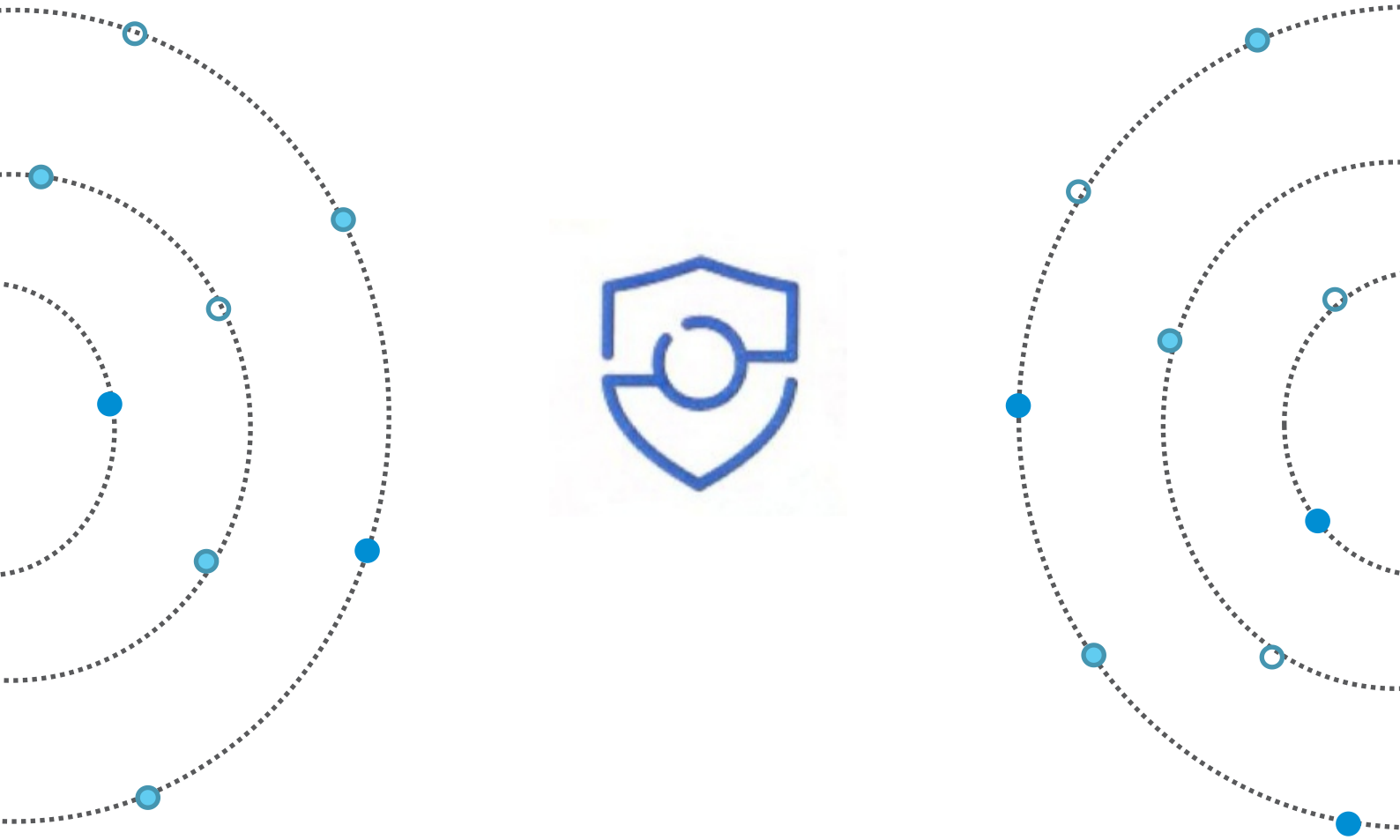
GDPR 执法案例全景白皮书

(2020)



合规创造价值
Compliance Creates Value

全球法律政策研究院
既是实干家，也是学术派

中兴通讯数据保护合规部

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，由此引发全球范围内关于个人数据保护立法、执法、企业合规、国际合作等的广泛讨论和深刻变革。公开信息统计显示， GDPR 生效的第一年，欧洲各国执法机构共作出了 48 项约 51,833,345 欧元的处罚决定，特别是从 2019 年初的谷歌天价罚款开始，呈现出执法全面开花势头，不断牵动和震撼着关注数据保护合规的群体。

2019 年下半年以来，执法机构打破 GDPR 生效初始期的慎重，接连开出了英航、万豪上亿欧元和奥地利邮政、Deutsche Wohnen SE 等上千万欧元的罚单，至今仍牢牢占据着 GDPR 生效以来的罚款榜单前列。进入 2020 年，GDPR 监管执法逻辑日渐清晰，随之以风险为导向的数据合规管控方法日益深化。针对欧洲经济区（EEA）数据保护执法态势深入研究和密切监测，有助于企业明确业务线合规治理要点，清晰国别线合规风控重点，有效预防提前预警。

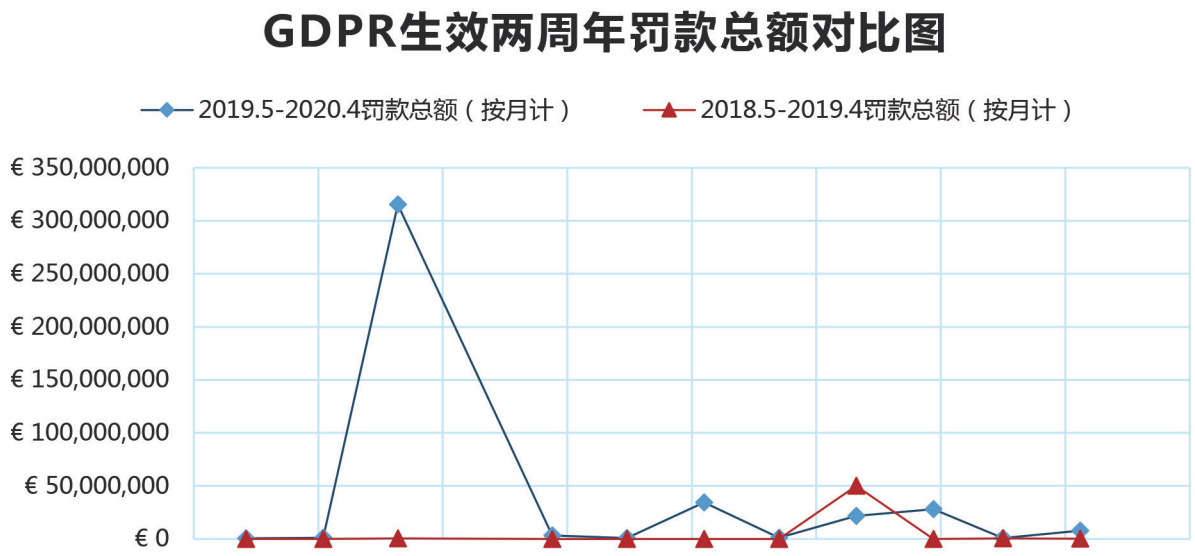
《GDPR 执法案例精选白皮书（2018-2019）》作为首部 GDPR 执法案例跟踪成果，自 2019 年 9 月发布以来受到了业内外专业人士和数据保护热心读者的广泛关注和全面好评。为了沿袭和承接白皮书“向前一步，只争第一”的实践精神，助力数据保护从业人员拨开 GDPR 执法迷雾，《GDPR 执法案例白皮书（2019.5-2020.5）》全新起航。

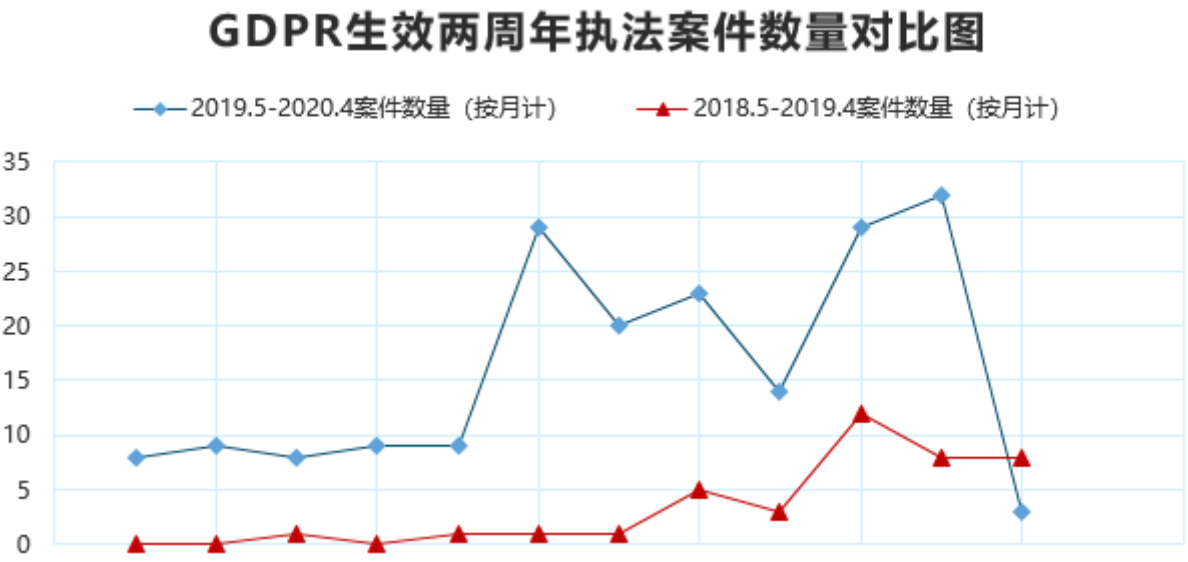
本白皮书延续了 2019 年 9 月发布的《GDPR 执法案例精选白皮书（2018-2019）》的框架和体例，从执法力度、执法依据两个角度进行分析，揭开 GDPR 生效进入第二年的执法面纱；从执法案件数量、执法金额两个维度进行对比，把握 GDPR 生效第一年试水期到第二年浅水区的执法趋势。本白皮书基于欧洲各国监管部门、研究机构、律所等公开信息，核心部分收录了发生于 2019 年 5 月 25 日至 2020 年 5 月期间的，涵盖了欧洲经济区 (European Economic Area, EEA) 19 个国家的 132 个执法案例。针对每个案例，除了从原有的处罚金额、依据、时间、案件事实、违规分析、合规启示六个方面进行呈现挖掘外，最新匹配了场景化红线，以期最大程度地发挥案例的借鉴启示意义，为企业的数据保护合规提供最鲜活的经验，最终实现数据合规创造价值。

目 录

执法态势数据统计

本部分根据所统计的案例信息，从时间、国家、违规类型、违规主体对相关案例进行归类整理，通过图表结合的方式，对 GDPR 执法趋势进行最直观清晰的呈现。

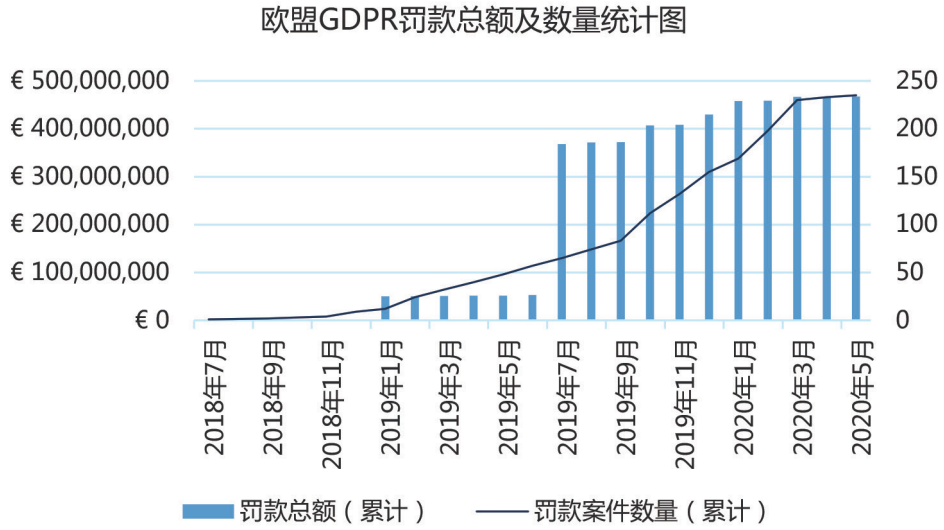




统计数据：时间

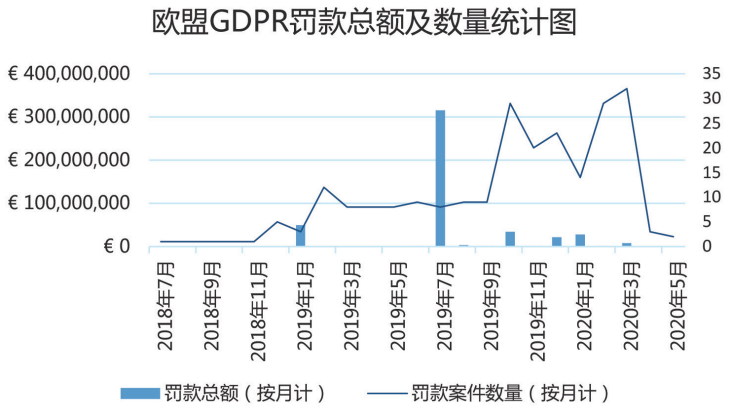
注意：仅考虑所收集的年份和月份的有效信息的罚款。

1. 每月罚款总额和总数（累计）：



年份及月份	罚款总额（至月）	罚款数量（至月）
2018年7月	€400,000	1
2018年9月	€400,300	2
2018年10月	€400,688	3
2018年11月	€420,688	4
2018年12月	€436,388	9
2019年1月	€50,437,276	12
2019年2月	€50,502,384	24
2019年3月	€50,964,684	32
2019年4月	€51,273,819	40
2019年5月	€51,833,345	48
2019年6月	€52,917,895	57
2019年7月	€368,275,670	65
2019年8月	€371,528,505	74
2019年9月	€372,435,028	83
2019年10月	€406,947,402	112
2019年11月	€408,062,202	132
2019年12月	€429,819,732	155
2020年1月	€457,930,442	169
2020年2月	€458,816,532	198
2020年3月	€466,677,568	230
2020年4月	€467,471,268	233
2020年5月	€467,487,468	235

2. 每月罚款的总数和数量（非累计）：



年份及月份	罚款总额（以月计）	罚款数量（以月计）
2018年7月	€400,000	1
2018年9月	€300	1
2018年10月	€388	1
2018年11月	€20,000	1
2018年12月	€15,700	5
2019年1月	€50,000,888	3
2019年2月	€65,108	12
2019年3月	€462,300	8
2019年4月	€309,135	8
2019年5月	€559,526	8
2019年6月	€1,084,550	9
2019年7月	€315,357,775	8
2019年8月	€3,252,835	9
2019年9月	€906,523	9
2019年10月	€34,512,374	29
2019年11月	€1,114,800	20
2019年12月	€21,757,530	23
2020年1月	€28,110,710	14
2020年2月	€886,090	29
2020年3月	€7,861,036	32
2020年4月	€793,700	3
2020年5月	€16,200	2

统计数据：罚款最高的国家（前10名）

以下统计数据显示了每个国家 / 地区（仅排名前 10 位的国家）判处的罚款总额和总数。

1. 罚款总额计：

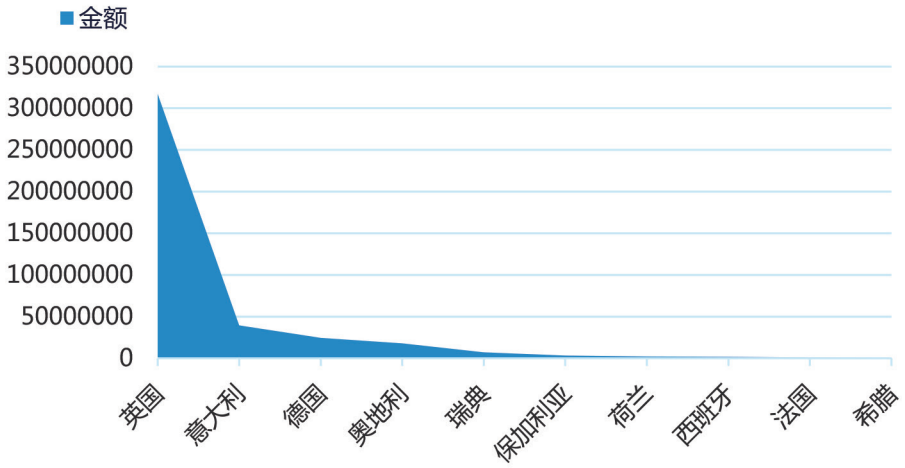


图1：执法金额前十国家对比图

	国家	罚款总额
	英国	€317,242,423（8次）
	意大利	€39,402,000（10次）
	德国	€24,460,407（7次）
	奥地利	€18,011,000（2次）

	国家	罚款总额
	瑞典	€7,072,330（4次）
	保加利亚	€3,174,480（13次）
	荷兰	€2,200,000（4次）
	西班牙	€1,826,070（63次）
	法国	€1,100,000（4次）
	希腊	€748,000（8次）

表1：执法金额前十国家统计表

2. 按罚款总数计：

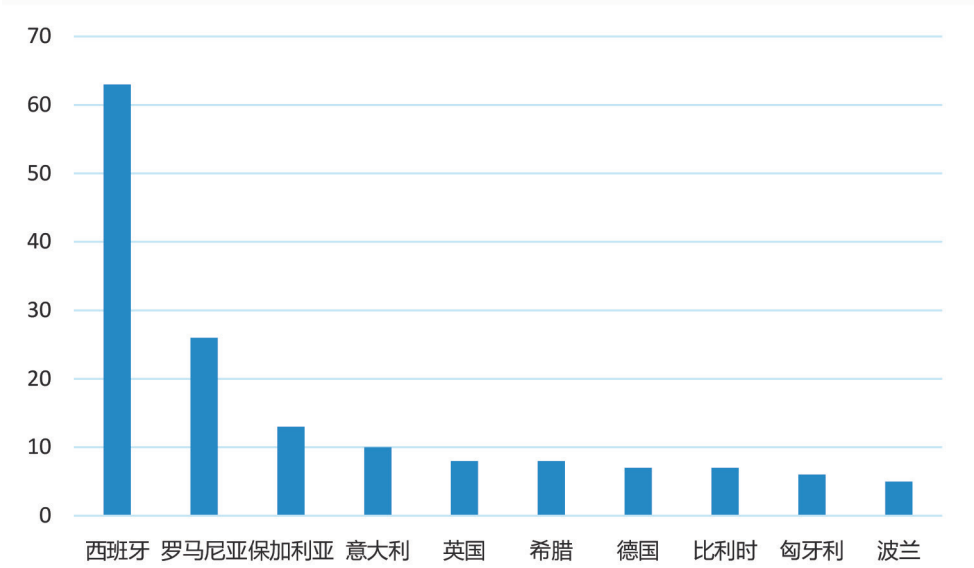


图2：执法数量前十国家对比统计图

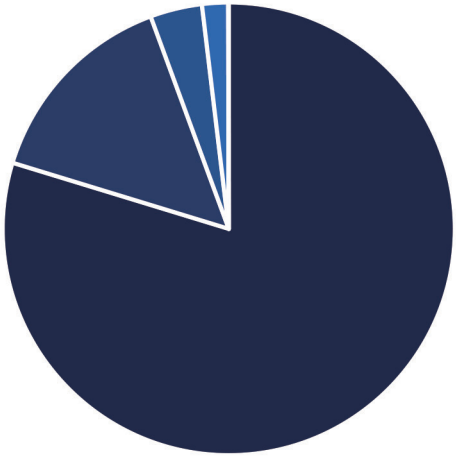
	国家	罚款数
	西班牙	63（总金额 € 1,826,070）
	罗马尼亚	26（总金额 € 499,706）
	保加利亚	13（总金额 € 3,174,480）
	意大利	10（总金额 € 39,402,000）
	英国	8（总金额 € 317,242,423）
	希腊	8（总金额 € 748,000）
	德国	7（总金额 € 24,460,407）
	比利时	7（总金额 € 89,000）
	匈牙利	6（总金额 € 31,366）
	波兰	5（总金额 € 710,380）

表2：执法数据前十国家统计表

统计信息：按违规类型分类的罚款

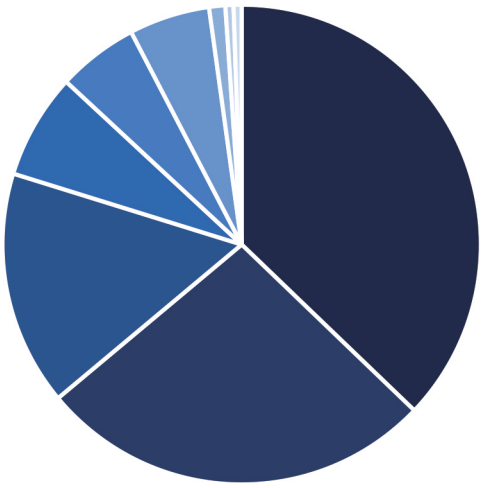
以下统计数据显示了每种 GDPR 违规类型已处的罚款总额以及罚款案件个数。

1. 罚款总额计：



	违反	罚款总额
	缺乏保障信息安全的技术和组织措施	€332,567,289（49次）
	数据处理的法律依据不足	€61,202,963（68次）
	违反数据处理基本原则	€15,495,940（29次）
	数据主体权利没有充分实现	€7,756,539（13次）
	DPO任命违反法律要求	€60,000（2次）
	与监督机构的合作不足	€59,911（10次）
	未充分履行信息义务	€31,300（10次）
	未签署数据处理协议	€9,380（1次）
	未充分履行数据泄露通知义务	€7,400（1次）

2. 按罚款总数计：



	违反	罚款数
	数据处理的法律依据不足	68（总金额 € 61,202,963）
	缺乏保障信息安全的技术和组织措施	49（总金额 € 332,567,289）
	违反数据处理基本原则	29（总金额 € 15,495,940）
	数据主体权利没有充分实现	13（总金额 € 7,756,539）
	未充分履行信息义务	10（总金额 € 59,911）
	与监督机构的合作不足	10（总金额 € 31,300）
	DPO任命违反法律要求	2（总金额 € 60,000）
	未充分履行数据泄露通知义务	1（总金额 € 9,380）
	未签署数据处理协议	1（总金额 € 7,400）

统计信息：最高罚款（前10名）

以下统计数据显示了每个数据控制者施加的最高罚款（仅前 10 名罚款）。

	控制者	国家	罚款[€]	违规类型	日期
1	British Airways	英国	204,600,000	技术和组织措施不足 无法确保信息安全	2019年07月08日
2	Marriott	英国	110,390,200	技术和组织措施不足 无法确保信息安全	2019年07月09日
3	TIM	意大利	27,800,000	数据处理的法律依据不足	2020年1月15日
4	Austrian Post	奥地利	18,000,000	数据处理的法律依据不足	2019年10月23日
5	Deutsche Wohnen SE	德国	14,500,000	不遵守一般数据处理原则	2019年10月30日
6	1 & 1 Telecom GmbH	德国	9,550,000	技术和组织措施不足 无法确保信息安全	2019年12月09日
7	Eni Gas e Luce	意大利	8,500,000	数据处理的法律依据不足	2019年12月11日
8	Google LLC	瑞典	7,000,000	数据主体权利的实现不足	2020年3月11日
9	Eni Gas e Luce	意大利	3,000,000	数据处理的法律依据不足	2019年12月11日
10	National Revenue Agency	保加利亚	2,600,000	缺乏保障信息安全的技术和组织措施	2019年8月28日

监管执法典型案例

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

Northern Ireland office：

电话：028 9027 8757 / 0303 123 1114

E-mail: ni@ico.org.uk

Wales office：

电话：0330 414 6421

Email: wales@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

※ 处罚金额

约为 2.04 亿欧元

※ 处罚依据

GDPR 第 32 条

※ 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。

※ 场景化红线

禁止采用安全系数低、过时的安全保障技术。禁止瞒报数据泄露事件。

02 万豪集团数据泄露事件

※ 处罚金额

1.1 亿欧元

※ 处罚依据

GDPR 第 32 条

※ 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。

※ 场景化红线

禁止采用安全系数低、过时的安全保障技术。

03 某企业缺乏适当的技术措施保障数据安全

※ 处罚金额

27,500 英镑（约 320,000 欧元）

※ 处罚依据

GDPR 第 5（1）（f）条，第 13 条，第 14 条，第 24（1）条，第 32 条

※ 处罚时间

2019/12/17

※ 案件事实概述

一家医药公司在其大楼后面的非密封容器中储存了约 50 万份文件，内含姓名、地址、出生日期、NHS 号码、医疗信息和处方，未能按照其数据处理程序将含有病人个人信息的文件撕碎后清理。同时其《隐私通知书》未明确说明数据控制者的身份、联系方式、处理数据的合法性基础等等。综合受影响数据主体范围、医疗健康数据敏感性等因素，监管机构作出了 27,500 欧元的罚款。

※ 违规分析

未采用适当的技术措施使数据免遭意外的丢失、销毁或破坏，违反了 GDPR 第 5（1）（f）、第 24 条（1）所规定的数据控制者的义务以及第 32 条规定的处理安全。此外未按照 GDPR 要求，向数据主体提供与数据处理有关的信息。

※ 合规启示

企业应采取适当的技术和组织措施以确保并证明数据处理是符合 GDPR 的规定，且应在必要情况下进行评估和更新。

※ 场景化红线

禁止将含有个人数据的文件存储在开放的容器中。

04 DSG Retail Limited数据泄漏事件

※ 处罚金额

500,000 英镑（约 580,000 欧元）

※ 处罚依据

1998 数据保护法案 Section 55A

※ 处罚时间

2020/1/9

※ 案件事实概述

ICO 调查发现，在 2017 年 7 月至 2018 年 4 月期间，攻击者在 DSG 的 CurrysPC 世界和 Dixons 差旅商店安装了 5390 分片恶意软件，并且在 DSG 检测到攻击之前的 9 个月内收集了个人数据。该公司未能确保该系统的安全，允许未经授权访问交易中使用的 560 万张支付卡详细信息和大约 1400 万人的个人信息（包括姓名、邮政编码、电子邮件地址等）。

※ 违规分析

未采用适当的技术措施保障其系统安全，造成了大量数据的非授权访问。

※ 合规启示

企业应采取适当的技术措施保障数据安全，防止数据非授权访问。

※ 场景化红线

禁止采取安全系数较低的安全保障技术。

05 CRDNN Limited非法拨打自动营销电话

※ 处罚金额

500,000 英镑（约 580,000 欧元）

※ 处罚依据

PECR 第 19 条，第 24 条

※ 处罚时间

2020/2/26

※ 案件事实概述

一家英国的发电机公司未经数据主体同意就拨打超过 193,606,544 项自动营销电话，且在该电话中未提供公司的信息或联系方式，也未提供拒绝接收此营销电话的方法，被英国数据保护监管机构处以 PECR（< 隐私和电子通信法 >）下的最高罚款 500,000 英镑。

※ 违规分析

未经数据主体同意就拨打营销电话，缺乏数据处理的合法性基础，并且没有提供退出的方式，违反了 PECR 第 19 条。未向数据主体提供拨打营销电话的主体的信息或联系方式，违反了 PECR 第 24 条。

※ 合规启示

企业应在具备合法性基础的情况下进行营销活动，应在营销活动中披露退出的方法以及企业的联系方式。

※ 场景化红线

禁止未经数据主体同意拨打营销电话。

06 Cathay Pacific Airways Limited数据泄露事件

※ 处罚金额

500,000 英镑（约 573,303 欧元）

※ 处罚依据

1998 数据保护法案 Section 55A

※ 处罚时间

2020/3/4

※ 案件事实概述

在 2014 年 10 月至 2018 年 5 月期间，国泰航空的计算机系统缺乏适当的安全措施，导致了包括护照号码等在内的个人数据泄露，直至 2018 年 3 月，其 4 个系统被攻击后才意识到这个问题，影响了大约 9,400,000 人。

※ 违规分析

未采用适当的技术措施使数据泄露，违反了数据的安全性和保密性原则。

※ 合规启示

企业应采取适当的技术措施保障数据安全，防止数据泄露。

※ 场景化红线

禁止采取安全系数较低的安全保障技术。

07 LeoKirk非法披露数据

※ 处罚金额

483 英镑（约 560 欧元）

※ 处罚依据

1998 数据保护法案 Section 55A

※ 处罚时间

2020/3/13

※ 案件事实概述

一名前社会工作者非法披露 16-18 岁弱势青年寄宿或寄养的相关信息给第三方，其中包含一些敏感个人数据。

※ 违规分析

未经授权将个人数据披露给其他第三方，违反了数据的安全性和保密性原则。

※ 合规启示

企业应采取适当的组织措施防止处理个人数据的员工泄露数据，同时应进行相应的数据保护培训提升员工意识。

※ 场景化红线

禁止非授权披露个人数据。

08 某企业非法拨打自动营销电话

※ 处罚金额

171,000 英镑（约 198,360 欧元）

※ 处罚依据

PECR 第 21 条、第 24 条

※ 处罚时间

2020/3/27

※ 案件事实概述

该公司以直接营销的目的使用公众电信服务，在未获取同意的情况下，直接呼叫了在 TPS（Telephone Preference Service Ltd）上至少提前 28 天注册了的用户，拨打超过 240,576 通电话。且在电话中意图隐瞒公司的真实名称，未向数据主体披露明确且真实的信息。

※ 违规分析

根据 PECR 第 21 条的使用公众电信服务进行营销的例外规定，未获得数据主体预先的同意，未提供拨打营销电话的主体的信息或联系方式，违反了 PECR 第 24 条。

※ 合规启示

企业应在具备合法性基础的情况下进行营销活动，应在营销活动中披露企业的联系方式。

※ 场景化红线

禁止未经数据主体同意拨打营销电话。

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

01 SERGIC数据泄露事件

※ 处罚金额

400,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 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。

※ 场景化红线

禁止对个人数据不采取足够的技术组织措施保证数据安全；

禁止超过数据处理目的所必要的期限存储个人数据。

02 ACTIVE ASSURANCES数据泄露事件

※ 处罚金额

180,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 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。

※ 场景化红线

禁止不采取任何访问限制措施导致个人数据的非授权方访问；

禁止对账户和密码设置较低的保密强度。

03 员工投诉某公司监控侵犯隐私事件

※ 处罚金额

20,000 欧元

※ 处罚依据

GDPR 第 5 (1) c) 条，第 12 条，第 13 条，第 32 条

※ 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）。

※ 违规分析

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。

场景化红线

禁止对员工进行持续和永久的监控。

04 某企业电话营销未充分实现数据主体权利

※ 处罚金额

500,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 13 条，第 14 条，第 21 条

※ 处罚时间

2019/11/21

※ 案件事实概述

该公司向现有或潜质客户拨打营销电话，尽管有几名投诉人直接告知来电者不希望再收到此类电话，并以邮寄信件的方式宣布不希望这样做，但该公司仍然拨打类似电话。 另外，该公司拨打电话时并未告知有关通话会被记录，或者只是告知了会记录对话，而不会向他们传达有关其个人数据处理的任何其他信息，例如处理的目的，数据控制者的身份或他们拥有的权利。同时，该公司对数据主体进行了过多的信息记录。监管机构还发现，该公司将个人数据跨境传输到位于欧洲经济区（“ EEA”）之外的呼叫中心，对此跨境转移行为没有提供足够的保障措施。

※ 违规分析

该公司未能有效地实施现有和潜在客户的退出请求，违反了关于数据主体拒绝权的相关规定；该公司记录相关通话的数据处理行为，未能履行充分性告知义务；该公司对数据主体进行了过多的信息记录违反了数据处理最小范围原则；该公司在进行个人数据的跨境传输过程中，未能履行向欧盟境外传输个人数据的相关义务。

※ 合规启示

公司在进行电话营销活动时必须做到：

1. 允许个人有效行使 GDPR 规定的权利，包括选择退出直接营销的权利，并制定流程以确保自动执行此类反对意见；

2. 在电话中告知个人相关权利，并通过按电话键或接收电子邮件为他们提供访问整个隐私政策的选项；

3. 向任何第三方运营商明确说明必须向消费者提供哪些信息以及可能记录哪些评论，并实施适当的自动化流程以防止在客户关系数据库中进行过多的术语记录；

4. 若将个人数据传输到 EEA 以外的任何数据中心，须采取适当的保护措施，例如订立标准合同条款。

※ 场景化红线

禁止在电话营销中对已经行使拒绝权的客户进行持续电话拨打；

禁止在未告知个人权利的情况下对个人数据的收集处理；

禁止超出范围收集记录数据主体的相关信息；

禁止在无相关适当保障措施的情况下将个人数据转移出欧盟境外。

3 保加利亚

COMMISSION FOR PERSONAL DATA PROTECTION

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

01 国家税务局数据泄露事件

※ 处罚金额

260,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 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。

※ 场景化红线

禁止采用安全系数低、过时的安全保障技术。

02 DSK银行数据泄露事件

※ 处罚金额

511,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 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。

※ 场景化红线

禁止采用安全系数低的技术措施。

03前雇主某公司未保障数据主体权利

※ 处罚金额

约 511 欧元

※ 处罚依据

GDPR 第 12（3）条、第 15（1）条

※ 处罚时间

2019/10/28

※ 案件事实概述

数据主体向其前雇主申请查阅其个人数据，要求前雇主提供其哪些个人数据在被处理，目的是什么，基于什么理由，在什么时期，另外还要求退还两份职业培训证书原件。前雇主拒绝回答，也没有退还原件。

※ 违规分析

前雇主在无合法理由的情况下拒绝了数据主体的请求，没有保障数据主体的权利。

※ 合规启示

企业应及时响应数据主体的权利请求，在无合法理由支撑的情况下不得拒绝。

※ 场景化红线

禁止在无合法理由的情况下拒绝数据主体的权利请求。

04 公用事业公司错误提供个人数据

※ 处罚金额:

5,110 欧元

※ 处罚依据

GDPR 第 5（1）（a）条、第 6（1）条

※ 处罚时间

2020/1/6

※ 案件事实概述

数据主体和其他债务人有相同的名字但是拥有不同的 PIN 码，保加利亚公用事业公司错误地将数据主体的 PIN 码提供给私人执法代理，随后被用于提起针对数据主体的强制执行诉讼，指控他未履行付款义务。在执行案件中，法警扣押了数据主体的工资，而数据主体由于非法处理而受到损害。

※ 违规分析

虽然表面上是一个数据错误地提供，其实是该公用事业公司在没有合法性基础的前提下处理了数据主体的数据。

※ 合规启示

企业应在合法性基础存在的前提下处理数据主体的个人数据。

※ 场景化红线

禁止在不满足合法性基础要求的情况下处理个人数据。

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 Molel.net数据泄露案

※ 处罚金额

2,800,000 波兰兹罗提（约 645,000 欧元）

※ 处罚依据

GDPR 第 5.1（f）条，第 32 条

※ 处罚时间

2019/9/10

※ 案件事实概述

Molel.net 采用了无效的身份验证措施和缺少监测异常在线行为等相关潜在威胁的制度，导致约 220 万人个人数据的未经授权的访问。并且部分泄露的数据被用于网络钓鱼，如通过在 SMS 消息中模拟 Molel.net 并利用客户下达订单的事实将款项存入银行帐户

※ 违规分析

Molel.net 未采用有效和适当的技术措施防止未经授权的访问，造成数据泄露，违反了 GDPR 第 5 条第 1 款（f）规定的完整性和保密性原则以及第 32 条规定的数据处理安全。

※ 合规启示

企业应采用安全系数较高的身份验证措施并且建立动态、有效的监测机制时刻防范数据泄露。

※ 场景化红线

禁止采用安全系数低的身份验证程序。

02 ClickQuickNow未保障同意撤销权的有效实现

※ 处罚金额

201,000 波兰兹罗提（约 46,302 欧元）

※ 处罚依据

GDPR 第 5（1）（a）条，第 7 条第 3 款，第 12 条第 2 款，第 17 条

※ 处罚时间

2019/10/16

※ 案件事实概述

该公司用一个包含有商业信息的链接进行同意的撤销，并未导致快速撤销的实现，并且在链接建立后，发给有意撤销同意的人的邮件具有误导性。此外，该公司强行要求有意撤销同意的数据主体说明其撤销同意的原因，如果未能说明原因，会导致撤销同意程序中断。对于已经要求删除其个人数据的客户而言，该公司还在继续处理其个人数据。

※ 违规分析

未采用合适的技术措施保障数据主体撤销同意与作出同意一样容易，违反了 GDPR 第 7 条第 3 款。未响应数据主体的被遗忘权请求权，违反了第 12 条第 2 款，第 17 条。对于数据主体要求删除的那部分个人数据而言已丧失合法性基础，该公司的处理行为违反了第 5（1）（a）的合法性原则。

※ 合规启示

企业应采取适当的措施保障同意的撤销与作出一样容易；

企业应积极地帮助数据主体行使其权利；

对于已经要求行使的删除权，应及时响应。

※ 场景化红线

禁止以任何方式阻止数据主体行使其权利。

03 Aleksandrów Kujawski市长未签署数据处理协议

※ 处罚金额

40,000 波兰兹罗提（约 9,214 欧元）

※ 处罚依据

GDPR 第 5（1）（a）条，第 5（1）（e）条，第 5（1）（f）条，第 5（2）条，第 28 条第 3 款

※ 处罚时间

2019/10/18

※ 案件事实概述

Aleksandrów Kujawski 市长没有与托管了市政府的公共信息公告（BIP）资源服务器的公司签订数据处理协议，也没有与另一家提供用于创建 BIP 软件及服务的公司达成这样的协议。内部的程序中没有规定BIP 中存储的数据的保存期限。没有市议会会议录音的副本，只能通过 YouTube 链接访问。

※ 违规分析

由于没有达成这样的协议，市长实施了无法律依据的共享个人数据的行为，这违反了处理合法性的原则，同时因缺乏作为协议保障的组织措施，违反了安全性和保密性原则。未规定数据的保存期限，违反了存储限制原则。没有录音的副本，因此在丢失存储在 YouTube 上的数据的情况下，该市将不会拥有记录，违反了完整性和保密性原则和责任原则。

※ 合规启示

企业应与数据处理者签订相应的数据处理协议保证数据处理的安全；

企业应针对不同的个人数据制定相应侧存储期限规范；

企业应做好数据备份。

※ 场景化红线

禁止不与数据处理者签订数据处理协议；

禁止不设置个人数据的保存期限；

禁止不对个人数据进行备份。

04 Danzig学校无合法性基础处理生物识别数据

※ 处罚金额

2,000,000 波兰兹罗提（约 460,714 欧元）

※ 处罚依据

GDPR 第 5 条，第 9 条

※ 处罚时间

2020/3/4

※ 案件事实概述

自 2015 年 4 月起，Gdansk 的一所学校在食堂入口处使用生物识别读取器来识别学生的指纹，以验证餐费的支付情况。在 2019-2020 学年，有 680 名学生使用生物识别读取器，而 4 名学生使用了替代生物识别系统的其他方法。家长已书面同意处理该指纹数据。

※ 违规分析

监管机构认为虽然学校强调获得了学生家长的同意，但是在学校和学生这样失衡的关系中，很难证明这个同意是自愿作出的，违反了 GDPR 第 5（1）（a）和第 9 条。此外生物识别数据的处理对于实现识别学生有权享用午餐的目标而言不是必不可少的。学校可以通过其他方式进行身份识别，而不会对学生的隐私造成太大的干扰，违反了 GDPR 第 5（1）（b）目的限制原则。

※ 合规启示

在选择合法性基础时，企业应充分考虑这个合法性基础是不是最合适以及是不是可以比较容易满足的；

在收集个人数据前，企业应论证该个人数据是实现处理目的所必要的。

※ 场景化红线

禁止选择不恰当的合法性基础；

禁止处理非处理目的所必需的个人数据。

05 Vis Consulting Sp. z o.o.与监督机构的合作不足

※ 处罚金额

20,000 波兰兹罗提（约 4,607 欧元）

※ 处罚依据

GDPR 第 31 条，第 58 条

※ 处罚时间

2020/3/9

※ 案件事实概述

监管机构想要对该公司进行相关调查，未能找到相关公司地址信息，在拨打了该公司的联系电话后，该公司的代表人回应调查将不会发生。

※ 违规分析

监管机构从该公司的行为判断其不愿意与监管机构展开合作，违反了 31 条和 58 条。

※ 合规启示

企业应与监管机构展开积极的合作，及时响应监管机构的要求。

※ 场景化红线

禁止以消极、对抗的态度与监管机构进行沟通。

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 Menzis使数据遭受未经授权的访问

※ 处罚金额

50,000 欧元

※ 处罚依据

GDPR 第 5.1（f）条，第 32 条

※ 处罚时间

2019/10/31

※ 案件事实概述

Menzis 是一家健康保险公司，虽然根据其权限控制政策，营销人员是不可以访问被保险人的医疗数据。但实际上这部分营销人员是可以访问的，目前尚未确定这些雇员实际上是否是将被保险人的医疗数据用于营销活动。 ※

※ 违规分析

Menzis 未能采取适当的技术措施使数据免遭受未经授权的访问，违反了 GDPR 第 5 条第 1 款（f）规定的完整性和保密性原则以及第 32 条规定的数据处理安全。

※ 合规启示

企业应采取适当的技术措施真正落实数据保护各项要求。

※ 场景化红线

禁止将权限控制只停留在政策层面。

02 UWV未采用高安保系数的身份验证

※ 处罚金额

900,000 欧元

※ 处罚依据

GDPR 第 5.1（f）条，第 32 条

※ 处罚时间

2019/10/31

※ 案件事实概述

UUWV（荷兰雇员保险机构），为荷兰社会事务和就业部授权的独立行政机构。机构的门户网站处理包括员工健康数据在内的敏感个人数据，还包括姓名、地址、BSN、财务状况和职业、是否被解雇、生育状况等数据。鉴于数据的敏感程度，访问必须通过多重身份认证，但 UWV 使用的是单因素身份认证，仅通过输入邮箱地址和密码就可实现访问，违反荷兰数据保护法（PDPA）的第 13 条及 GDPR 有关规定。

※ 违规分析

UWV 未能采取适当的技术和组织措施保护雇员数据的安全，违反了 GDPR 第 5 条第 1 款（f）规定的完整性和保密性原则以及第 32 条规定的数据处理安全。

※ 合规启示

企业应采取多重因素身份验证等适当的技术措施来保证访问安全。

※ 场景化红线

禁止采取安全系数较低的身份验证技术。

03 荷兰皇家网球协会数据处理法律依据不足

※ 处罚金额

525,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/3/3

※ 案件事实概述

荷兰皇家网球协会（KNLTB）是荷兰网球运动和网球俱乐部的总括组织。KNLTB 将从 35 万名会员处收集的包括姓名、住所、电话号码等在内的个人数据出售给赞助商。在其 2005 年的章程里促进网球比赛的练习以及荷兰网球运动的发展。其次，收集注册数据（个人数据），以提供给第三方。但是没有明确说明第三方的类别。2007 年修改为为直接营销目的提供给赞助商。在其 2018 年的隐私声明中也有类似描述，并将合法性基础规定为合法利益。

※ 违规分析

对于 2007 年前收集的个人数据，监管机构认为数据处理目的没有很好地进行定义，因此 KNLTB 的成员无法由此推断他们个人数据也将提供给赞助商进行直接营销活动。因此，KNLTB 的行为违反了 GDPR 第 5 条第 1 款（a）的合法性原则要求，不具备数据处理的合法性基础。对于 2007 以后收集的个人数据，监管机构认为 KNLTB 所举证的“给会员增值”和“降低会员减少产生的损失”不符合 GDPR 第 6 条第 1 款（f）所规定的“合法利益”，缺乏紧迫性，因此这部分数据处理也不具备充分的合法性基础，违反了 GDPR 第 5 条第 1 款（a）的合法性原则要求。

※ 合规启示

企业应充分理解 GDPR 第 6 条第 1 款所规定的 6 个合法性基础，选择适当的进行数据处理；

对于超出原有目的进行的处理应按照 GDPR 第 6 条第 4 款的要求进行考虑。

※ 场景化红线

禁止选取不恰当的合法性基础作为数据处理的依据。

04 某组织非法处理员工特殊类型个人数据

※ 处罚金额

725,000 欧元

※ 处罚依据

GDPR 第 5 条，第 9 条，第 12 条、第 13 条

※ 处罚时间

2020/4/30

※ 案件事实概述

该组织要求员工必须扫描登记指纹用于考勤打卡。自 2017 年 1 月 23 日起，共计采集了 337 名员工的指纹数据，其中 2018 年 5 月 25 日以后共有 87 名员工指纹数据被捕获并存储，且该组织未能遵照透明原则向员工提供法律要求的关于数据处理行为的信息，劳动合同和员工手册中并未包含任何关于使用指纹数据的说明。此外，离职员工的指纹信息尽管会被阻止访问并且不再在软件程序和扫描仪中处于活跃状态，但是仍然会被保留。

※ 违规分析

没有合法性基础处理特殊类别个人数据；未能遵照透明原则向员工提供法律要求的关于数据处理行为的信息；未删除离职员工的指纹数据，违反存储限制原则。

※ 合规启示

企业基于管理目的需要处理员工诸如指纹、面部信息等特殊类型个人数据时，应先进行充分的必要性测试、利益平衡测试，判断此类管理措施是否能够实施、在什么程度下可以实施。如果经评估后判断可以实施，则应当充分地向数据主体披露与数据处理活动有关的信息。

※ 场景化红线

严禁没有合法性基础处理特殊类型个人数据。

6 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 AVON COSMETICS非法处理个人数据

※ 处罚金额

60,000 欧元

※ 处罚依据

GDPR 第 6 条

※ 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。

※ 场景化红线

禁止未充分验证请求人的身份即对相关个人数据进行更改处理。

02 沃达丰将个人数据发送给非授权第三人

※ 处罚金额

60,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条

※ 处罚时间

2019/10/23

※ 案件事实概述

Vodafone 向服务订阅方发送了其服务相关的发票，发送的发票中还包含未知第三方的发票数据。

※ 违规分析

Vodafone 将基于服务所处理的个人数据相关内容发送给非授权的第三方，根据调查表明 Vodafone 未能采取足够的技术组织措施保证数据处理的完整性和保密性，从而将个人数据未经许可泄露给其他人。

※ 合规启示

企业应当采取必要的技术和组织措施，保障数据处理的安全水平，避免将个人数据未经许可

泄露给其他人。

※ 场景化红线

禁止将个人数据未经许可泄露给他人。

03 沃达丰数据处理的法律依据不足

※ 处罚金额

36,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2019/10/25

※ 案件事实概述

该投诉人的个人数据是他的女儿声称根据他的授权提供给 Vodafone 的。他接到了 Vodafone 的电话，声称已经为其开通了服务，但他表示拒绝。然而，Vodafone 忽视了他的请求，继续向他提供服务并要求他付款，因此 Vodafone 未经他同意处理了他的个人数据。

※ 违规分析

投诉人的个人数据已在 Vodafone 的文件中注册并经过处理以开具与投诉人相关的服务的发票。因此，这是在未授权的情况下进行的个人数据的处理。 最终，被告没有提供任何文件或证据表明在这种情况下已进行了最低限度的尽职调查，以验证对话者确实是声称要订阅相关服务的人。因此相关处理未获得数据主体的同意，这违反了数据处理合法性原则。

※ 合规启示

企业在为客户开通相关服务时，需要对请求人与业务开通人进行必要的身份核查，防止个人数据的非授权处理，从而影响数据处理的合法性。

※ 场景化红线

禁止在寻求获得数据主体的同意时未核查作出同意相关人的身份即开始进行数据处理。

04 Jocker Premium Invex数据处理的法律依据不足

※ 处罚金额

6,000 欧元

※ 处罚依据

GDPR 第 6 条

※ 处罚时间

2019/10/31

※ 案件事实概述

该公司在注册为本地人口普查组织后，利用名字、姓氏和邮政地址等数据向个人发送了邮政信件，邀请其参加在 2019 年 1 月 10~11 日由该公司主办的在宣传手册中列明的特定地点的商事活动，这属于广告和商业邀约。

※ 违规分析

该公司已注册为人口普查组织，只能基于其人口普查的目的收集处理数据。其利用之前收集的姓名、邮政地址，向数据主体发送商业广告类信息，属于无合法性基础处理个人数据，违反了数据处理的合法性原则。

※ 合规启示

企业基于某个目的进行数据处理不符合最初收集个人数据的目的时，应当寻求基于此目的下进行数据处理的新的合法性基础。

※ 场景化红线

禁止在无合适的合法性基础下超出最初收集个人数据的目的处理个人数据。

05 某公司未充分提供关于其数据处理的相关信息

※ 处罚金额

900 欧元

※ 处罚依据

GDPR 第 13 条

※ 处罚时间

2019/11/7

※ 案件事实概述

该公司未能根据 GDPR 第 13 条，在其数据保护声明中没有提供关于数据收集的准确信息。

※ 违规分析

该公司作为数据控制者未充分提供关于其数据处理的相关信息，违反了 GDPR 第 13 条关于数据控制者履行充分性告知的义务。

※ 合规启示

企业应当在获取个人数据的同时向数据主体提供详细准确的数据处理信息，具体应至少包括数据控制者信息、DPO 信息、数据处理目的和合法性基础、数据接受者及其类别（如有）、数据跨境转移情况、数据存储期限、数据主体权利等。

※ 场景化红线

禁止在收集处理个人数据时未向数据主体履行关于其个人数据处理的具体准确的信息告知义务。

06 工会委员会非授权公开投诉人个人数据

※ 处罚金额

3,000 欧元

※ 处罚依据

GDPR 第 6 条

※ 处罚时间

2019/11/13

※ 案件事实概述

工会委员会在未经投诉人同意的情况下，为了召开会议，通过电子邮件向 400 名工会成员发送了申诉人的个人数据，包括她的住址、家庭关系、怀孕状况和正在遭受的辱骂和骚扰案件的具体情况。

※ 违规分析

工会委员会在无相关合法性基础的情况下将投诉人的个人数据通过电子邮件发送给其他工会成员的行为，违反了数据处理的合法性要求。

※ 合规启示

企业在处理个人数据时，应当确保存在适当的合法性基础，尤其在涉及特殊类型个人数据的情况下，无相关合法性基础不能向其他非授权人员披露。

※ 场景化红线

禁止无适当合法性基础将个人数据披露给非授权的第三方。

07 Telfónica处理用户个人数据违反准确性原则

※ 处罚金额

30,000 欧元

※ 处罚依据

GDPR 第 5（1）（d）条

※ 处罚时间

2019/11/14

※ 案件事实概述

Telfónica 向投诉人收取了非他所有的电话号码有关的各种费用。其原因是，申诉人的银行账户与另一名 Telfónica 客户不当关联，导致相关费用从申诉人的账户中扣除。

※ 违规分析

该公司处理其客户的个人数据发生错误，导致向错误的服务对象收费，其处理个人数据违反了准确性原则。

※ 合规启示

企业应当采取一些合理的措施确保与数据处理目的相悖的错误数据被及时清除和更正。

※ 场景化红线

禁止在对相关账单发票未进行核对就发送给

客户。

08 广播电视公司数据泄漏事件

※ 处罚金额

60,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 处罚时间

2019/11/19

※ 案件事实概述

该广播电视公司和工会向 AEPD 报告了一起数据泄露事件。该事件是因为该公司丢失了六个包含个人数据的未加密 USB 移动闪存设备，影响到大约 11,000 人，其中包括身份识别数据、就业数据、刑事定罪数据和健康数据。

※ 违规分析

该公司针对个人数据的处理未能采取适当的技术和组织措施，使得存储大量个人数据的移动设备在未加密的情况下发生丢失，造成数据泄露风险，违反了数据处理的安全性要求。

※ 合规启示

企业应当采取必要的技术和组织措施，保障数据处理的安全水平。应当避免将个人数据存储在类似于移动闪存设备这类移动性较强的设备中，即使需要通过这样的设备便捷化传输数据，也要在完成传输后及时删除，同时应当对这类设备进行加密。

※ 场景化红线

禁止在安全保障水平较低的环境下利用移动设备对个人数据进行未加密的传输和存储。

09 体育酒吧视频监控设备安装违反最小范围原则

※ 处罚金额

6,000 欧元

※ 处罚依据

GDPR 第 5（1）（c）条

※ 处罚时间

2019/11/19

※ 案件事实概述

体育酒吧经营视频监控系统，其中摄像机的观察角度延伸到公共交通区域。

※ 违规分析

该体育酒吧安装的视频监控设备所监控的范围超出了数据处理目的所必须的最小范围，违反了最小范围原则。

※ 合规启示

公共空间图像的处理一般只能由负责安全管理的权力机关进行，而私人空间中安装的摄像头除非是因实现监控保障目的而至关重要，或者由于其位置而无法避免，一般而言不应进行不必要的数据处理，特别是不能影响公众、邻近建筑物和车辆周围的空间。也就是说，私人监控设备只可以例外地捕获为预定安全目的所必需的公共区域的最小部分。

※ 场景化红线

安装的视频监控设备禁止将观察角度延伸到社会公共空间。

10 供水服务公司数据处理的法律依据不足

※ 处罚金额

60,000 欧元

※ 处罚依据

GDPR 第 6 条

※ 处罚时间

2019/11/21

※ 案件事实概述

该公司是一家供水服务公司，其与投诉人之间有供水合同。但该公司未经客户（投诉人）同意，

由第三方处理（修改）合同中包含的客户的个人数据。相关修改是针对个人财产的承租人，该承租人作为供水服务的直接利益相关人。

※ 违规分析

该公司对供水服务合同中的客户个人数据的修改处理，未获得数据主体的同意，无其他合适的数据处理的合法性基础，违反了数据处理的合法性原则。

※ 合规启示

企业处理个人数据应当有适当的合法性基础。对于与客户签署的服务合同，在合同有效期间，对合同中的个人数据的变更等处理需要获得客户（数据主体）的同意。

※ 场景化红线

禁止在无适当合法性基础的情况下对与自然人签署的合同中的个人数据进行变更、修改或其他处理。

11 Cerrajeria Verin S.L.未充分履行信息告知义务

※ 处罚金额

1,500 欧元

※ 处罚依据

GDPR 第 13 条

※ 处罚时间

2019/12/3

※ 案件事实概述

该公司未在其网站上公布的隐私政策中提供有关其数据处理活动的准确信息。

※ 违规分析

该公司的隐私政策没有按照 GDPR 第 13 条的要求公布数据主体所应获得的具体信息。

※ 合规启示

企业的隐私政策应当按照 GDPR 第 13 条及 / 或 14 条的要求公布数据主体所应获得的具体信息。

※ 场景化红线

禁止不完整、不明确地向数据主体披露其应当提供的数据处理信息。

12 保险公司数据处理的法律依据不足

※ 处罚金额

5,000 欧元

※ 处罚依据

GDPR 第 6 条

※ 处罚时间

2019/12/3

※ 案件事实概述

该保险公司在未征得同意的情况下，发送了关于保险广告方面的电子邮件，该邮件中带有相关链接推送，直接指向自己网站的注册界面。尽管没有任何证据表明收到广告邮件的个人与该公司有任何服务上的关系或往来。

※ 违规分析

该公司进行邮件广告推送的数据处理行为无适当的合法性基础，违反了数据处理的合法性原则。

※ 合规启示

企业处理个人数据应当有适当的合法性基础。在进行邮件广告推送前需要确保所收集的邮件地址是能够基于此营销目的进行处理，即需要有确定的合法性基础，比如数据主体的有效同意等。

※ 场景化红线

禁止在无适当合法性基础的情况下发送广告类邮件推送。

13 Megastar SL设置的视频监控超越最小必要范围

※ 处罚金额

1,600 欧元

※ 处罚依据

GDPR 第 5（1）（a）（c）条，第 13 条

※ 处罚时间

2019/12/10

※ 案件事实概述

该公司运营了一个视频监控系统，但是摄像机的观察角度不必要地延伸到了公共交通区域，此外没有附加数据保护通知的标志。

※ 违规分析

该公司可以基于安全考虑在公司内部某些地方设置视频监控系统，但是对于公司外部的公共空间的监控超越了原本的数据处理目的，违反了最小范围原则。此外没有张贴数据保护的标志提示数据主体关于视频监控所涉及的数据处理的详细信息，违反了透明性原则。

※ 合规启示

企业可以出于安全的考虑设置视频监控系统，但应注意与公共利益、员工利益与权利的平衡，选取恰当的地点进行监控。同时应当注意设置相关数据保护通知保障数据主体的知情权。

※ 场景化红线

禁止超越数据处理目的最小必要范围设置视频监控。禁止以隐蔽的方式设置视频监控。

14 某企业用抄送所有人的方式进行营销信息推送

※ 处罚金额

5,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 处罚时间

2019/12/10

※ 案件事实概述

该公司向多个收件人发送广告电子邮件，每位收件人都可以看到所有其他收件人的电子邮件地址，因为收件人地址被放在抄送一栏，并非是密送。

※ 违规分析

该公司在进行营销活动时未充分考虑到各个收件人邮箱地址的保密性，将其披露给其他收件人，同时加大了邮箱地址向更大范围泄露的风险。

※ 合规启示

企业在进行营销信息的批量发送时，应注意每位收件人的个人信息保密性和安全性，采取密送等方式进行。

※ 场景化红线

禁止以发送或抄送所有数据主体的形式进行营销活动。

15 沃达丰向错误的收件人发送了含有个人数据的合同

※ 处罚金额

44,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条

※ 处罚时间

2020/1/7

※ 案件事实概述

该公司向错误的收件人发送了一份包含他人姓名、地址和电话号码等的个人数据合同。

※ 违规分析

该公司错误地发送个人数据，破坏了个人数据的保密性。

※ 合规启示

企业应采取适当的技术和组织措施避免错误发送个人数据的事件发生。

※ 场景化红线

禁止将个人数据发送给不匹配的数据主体。

16 某企业数据处理的法律依据不足

※ 处罚金额

10,000 欧元

※ 处罚依据

GDPR 第 6（1）（a）条

※ 处罚时间

2020/1/7

※ 案件事实概述

Asociación de Médicos Demócratas 处理了其成员的个人资料，尽管该协会曾收到警告说，它在未经数据主体同意的情况下进行了处理。该机构认为数据主体以口头形式提供了数据，尽管在默示的基础上并未明确地予以同意，但是并不反对广告的投放。

※ 违规分析

该机构机构获得的同意是无效的，因此该机构在缺乏合法性基础的情况下处理了数据主体的个人数据。

※ 合规启示

如果企业以同意为数据处理的合法性基础，则应确保获得的同意是有效的。

※ 场景化红线

禁止以无效的同意作为数据处理的依据。

17 沃达丰未及时响应监管机构需求

※ 处罚金额

3,000 欧元

※ 处罚依据

GDPR 第 58 条

※ 处罚时间

2020/1/9

※ 案件事实概述

西班牙数据保护监管机构要求该企业在 2019 年 11 月 12 日前提供所需要的信息，但是该企业未在规定的时间内提供。

※ 违规分析

各数据保护监管机构有权命令数据控制者或数据处理者、其代表人（如果有）提供其履行职责所必要的所有信息，因此企业在收到监管机构的信息需求时应及时进行配合。

※ 合规启示

企业应积极配合、及时响应监管机构的调查需求。

※ 场景化红线

禁止忽略或延迟监管机构的调查需求。

18 某企业视频监控超越最小必要范围

※ 处罚金额

3,600 欧元

※ 处罚依据

GDPR 第 5（1）（c）条

※ 处罚时间

2020/1/14

※ 案件事实概述

该店老板安装了一个视频监控系统，除店内，还对人行道以及公共空间进行了监控拍摄。

※ 违规分析

店老板可以出于安全考虑在店内某些地方设置视频监控系统，但是对于店铺外部的公共空间的监控超越了原本的数据处理目的，违反了最小范围原则。

※ 合规启示

企业可以出于安全的考虑设置视频监控系统，但应注意与公共利益、员工利益与权利的平衡，选取恰当的地点进行监控。

※ 场景化红线

禁止超越数据处理目的最小必要范围设置视频监控。

19 Xfera Moviles S.A.非法处理个人数据

※ 处罚金额

60,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/2/3

※ 案件事实概述

XFERA MOVILES 违反了 GDPR 的第 6 条第 1 款，因为该公司非法处理了包括银行详细信息，客户地址和数据主体名称在内的数据。

※ 违规分析

该公司未经同意处理数据主体的个人数据，违反了 GDPR 关于同意的规定，不具备数据处理的合法性基础。

※ 合规启示

禁止在数据处理合法性依据不足的情况下处理数据主体的个人数据。

※ 场景化红线

禁止在数据处理合法性依据不足的情况下处理数据主体的个人数据。

20 沃达丰未经授权处理个人数据

※ 处罚金额

75,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/2/3

※ 案件事实概述

沃达丰在数据主体不知情或未同意的情况下与第三方签署了一项电话订购转移合同。

※ 违规分析

沃达丰在数据主体不知情或未同意的情况下与第三方签署了一项电话订购转移合同，不具备数据处理的合法性基础。

※ 合规启示

向第三方披露数据主体的个人数据应提前获取数据主体同意。

※ 场景化红线

禁止在数据主体不知情或未同意的情况下向第三方披露数据主体的个人数据。

21 沃达丰未经授权处理个人数据

※ 处罚金额

60,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/2/3

※ 案件事实概述

数据主体投诉称，他曾收到沃达丰西班牙公司的一封电子邮件，其中包含该数据主体从未要求的电话账单，导致其个人数据未经他的同意被处理。数据主体的个人数据被合并到 VodafoneEspaña 的信息系统中，而 Vodafone 不能证明数据主体同意收集和随后处理其个人数据。

※ 违规分析

该公司未经同意处理数据主体的个人数据，违反了 GDPR 关于同意的规定，不具备数据处理的合法性基础。

※ 合规启示

处理个人数据应当经过数据主体授权。

依据数据主体同意处理个人数据，应当做好记录举证。

※ 场景化红线

未经数据主体授权，禁止处理其个人数据，如电话账单。

22 沃达丰错误发送个人数据

※ 处罚金额

50,000 欧元

※ 处罚依据

GDPR 第 5 条

※ 处罚时间

2020/2/3

※ 案件事实概述

一位数据主体投诉称沃达丰向其邻居发送了载有其个人数据的发票，如姓名、身份证和地址。

※ 违规分析

该公司错误地发送个人数据，破坏了个人数据的保密性。

※ 合规启示

企业应采取适当的技术和组织措施避免错误发送个人数据的事件发生。

※ 场景化红线

禁止将个人数据发送给不匹配的数据主体。

23 Automoción雇员非法处理个人数据

※ 处罚金额

800 欧元

※ 处罚依据

GDPR 第 5（1）（a）条，第 6（1）条

※ 处罚时间

2020/2/3

※ 案件事实概述

该公司一名雇员利用职务之便获取了某女同事的个人资料，在色情门户网站上制作了一个关于该女同事的假档案，其中包括她的详细联系方式、照片等。根据这份资料，数据主体受到了看到了这些资料后想要联系她的人的骚扰。

※ 违规分析

代表公司处理个人数据的员工对所接触到的其他人的个人数据进行了滥用，不具备合法性基础。

※ 合规启示

企业应加强数据保护培训，提升代表公司处理个人数据的员工的数据保护合规意识，避免员工滥用权限。

※ 场景化红线

禁止员工利用职务之便滥用他人的个人数据。

24 某企业数据处理的合法性基础不足

※ 处罚金额

6,670 欧元

※ 处罚依据

GDPR 第 5（1）（a）条，第 6（1）条，第 21 条

※ 处罚时间

2020/2/3

※ 案件事实概述

数据主体并非是该公司的客户，但该公司未获得数据主体同意向其发送广告消息，并且在数据主体拒绝收到此类广告消息后仍然继续进行发送。

※ 违规分析

在缺乏合法性基础的情况下，该企业处理了该数据主体的数据，并且没有响应数据主体的拒绝权。

※ 合规启示

企业应在具备合法性基础的情况下进行营销信息的发送，并且应有效响应数据主体的拒绝权。

※ 场景化红线

禁止企业在没有合法性基础的前提下处理数据主体的个人数据。

25 沃达丰向前客户寄送发票

※ 处罚金额

75,000 欧元

※ 处罚依据

GDPR 第 5（1）（a）条，第 6（1）条

※ 处罚时间

2020/2/3

※ 案件事实概述

数据主体是该公司的前客户，在解除服务关系后仍继续收到发票通知，但当时既没有合同关系，也没有任何逾期付款。沃达丰表示，由于技术失误造成了邮寄错误。

※ 违规分析

在合同关系已经解除，又不存在其他合法性基础的情况下，该企业处理了该数据主体的数据。

※ 合规启示

在与客户的合同关系已经终止的情况下，企业应在具备新的合法性基础之后才能处理其个人数据。

※ 场景化红线

禁止企业在没有合法性基础的前提下处理数据主体的个人数据。

26 某企业数据处理的合法性依据不足

※ 处罚金额

20,000 欧元

※ 处罚依据

GDPR 第 5（1）（a）条，第 6（1）条

※ 处罚时间

2020/2/3

※ 案件事实概述

拥有该公司会员卡的一名会员要求退出忠诚度计划，并撤回关于公司处理其个人数据的同意。但是由于错误的操作该公司继续向此数据主体发送了邮件。

※ 违规分析

在数据主体已经撤回同意，又不存在其他合法性基础的情况下，该企业处理了该数据主体的数据。

※ 合规启示

在数据主体已经撤回同意的情况下，企业应在具备新的合法性基础之后才能处理其个人数据。

※ 场景化红线

禁止企业在没有合法性基础的前提下处理数据主体的个人数据。

27 某餐厅使用视频监控违反最小化原则

※ 处罚金额

1,500 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/2/4

※ 案件事实概述

长崎自助餐厅将监控摄像机设置于餐厅外的公共空间，以不成比例的方式获取公共人行道的图像，影响了在人行道上自由行走的行人的权利。

※ 违规分析

处理个人数据应当遵守数据最小化原则，在充分、相关且仅限于必要的范围内处理，长崎自助餐厅以不成比例的方式获取公共人行道上行人的图像，违反了数据最小化原则。　　合规启示

在视频监控场景中，应当遵守数据最小化原则，在充分、相关且必要范围内设置监控范围和时间。

※ 场景化红线

在视频监控场景中，禁止将监控范围扩大到不必要的范围，禁止超出必要范围收集个人数据。

28 西班牙沃达丰未经同意处理客户个人数据

※ 处罚金额

60,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/3/4

※ 案件事实概述

数据主体收到某运营商的几条短信，称其已激活新的服务合同。原因是西班牙沃达丰的一名员工未经数据主体授权同意，以客户的名义与第三方运营商签订了合同。沃达丰不能证明其取得了客户的同意或有其他足够的合法性基础处理个人数据。

※ 违规分析

数据处理应当具备合法性基础，西班牙沃达丰未经数据主体授权同意也没有其他合法性基础处理客户个人数据，违反了数据处理的合法性原则。

※ 合规启示

企业在进行数据处理前务必要确保具备相应的合法性基础。

※ 场景化红线

严禁在缺乏合法性基础或法律依据不足情况下处理个人数据。

29 Grupo未经授权披露个人数据

※ 处罚金额

2,500 欧元

※ 处罚依据

GDPR 第 5（1）（f）条

※ 处罚时间

2020/2/14

※ 案件事实概述

房地产公司从财房地产经纪人处获得了有兴趣的买家的联系电子邮件，并将获得的数据向第三方披露。

※ 违规分析

该公司在没有合法性基础的情况下通过电子邮件向未经授权的第三方传播个人数据，违反了 GDPR 完整性和保密性原则的规定。

※ 合规启示

处理个人数据，应当具备合法性基础。

※ 场景化红线

未经数据主体授权或不具备其他合法性基础，禁止向第三方披露其个人数据。

30 某学校未经授权处理个人数据

※ 处罚金额

3,000 欧元

※ 处罚依据

GDPR 第 6 条

※ 处罚时间

2020/2/14

※ 案件事实概述

学校将孩子的图片以及其他个人数据不正当转移给第三方，第三方在没有法律依据的情况下发布孩子的图片。孩子的家长已明确表达不同意上述转移行为。

※ 违规分析

该学校未经监护人同意处理儿童的个人数据，违反了 GDPR 关于同意的规定，不具备数据处理的合法性基础。

※ 合规启示

处理儿童个人数据，应当事先征得其监护人同意。

※ 场景化红线

未经数据主体授权，禁止向第三方披露其个人数据。

31 IberdoaClientes电力公司未经授权处理个人数据

※ 处罚金额

80,000 欧元

※ 处罚依据

GDPR 第 6 条

※ 处罚时间

2020/2/14

※ 案件事实概述

IberdoaClientes 是一家电力公司，未经数据主体同意，终止了和数据主体的原合同，与数据主体签订了三份新合同，非法处理其个人数据。除了这项罚款外，AEPD 还根据西班牙旧的《数据保护法》处以另外 50000 欧元的罚款。

※ 违规分析

该公司数据处理没有合法性基础，未经数据主体同意且不符合其他合法利益。

※ 合规启示

与数据主体订立服务合同应当事先征得数据主体授权。

※ 场景化红线

未经数据主体授权，禁止处理其个人数据用于订立服务合同。

32 西班牙沃达丰违反数据安全保障义务

※ 处罚金额

42,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条

※ 处罚时间

2020/2/14

※ 案件事实概述

申诉人在访问他的个人沃达丰空间时，由于沃达丰匹配了另一位客户的身份证号码，申诉人可以看到该客户的个人数据。申诉人通知沃达丰后，仍未纠正。

※ 违规分析

该公司未能采取必要的技术措施保护相关个人数据不被非法处理，未能满足数据处理安全性要求，违反了数据处理完整性和保密性原则。

※ 合规启示

收到数据主体更正个人数据的要求时，应当及时处理、反馈。应当采取适合的技术和组织措施保障数据的安全性。

※ 场景化红线

禁止无视、拖延处理收到的数据主体更正个人数据的要求。

33 Mymoviles违反公开透明原则

※ 处罚金额

1,500 欧元

※ 处罚依据

GDPR 第 13 条

※ 处罚时间

2020/2/18

※ 案件事实概述

AEPD发现该公司未在其网站上发布隐私声明，并且其法律声明并未充分表明自己的身份。

※ 违规分析

该公司未向数据主体公开隐私声明，违反了公开透明原则。

※ 合规启示

收集处理个人信息的网站应当发布隐私声明，向数据主体公开数据收集处理规则，并表明自己的身份。

※ 场景化红线

网站上不得缺失隐私声明；

在隐私声明中不得隐瞒或不充分说明控制者身份。

34 CASA使用视频监控违反最小化原则

※ 处罚金额

6,000 欧元

※ 处罚依据

GDPR 第 5（1）（c）条

※ 处罚时间

2020/2/25

※ 案件事实概述

Casa Gracio Operation（简称 CASA）公司在一家酒店内使用闭路电视摄像机，该摄像机还拍摄了酒店外的公路，以不成比例的方式获取公共人行道的图像，影响了在人行道上自由行走的行人的权利。

※ 违规分析

处理个人数据应当遵守数据最小化原则，在充分、相关且仅限于必要的范围内处理，该公司以不成比例的方式获取公共人行道上行人的图像，违反了数据最小化原则。

※ 合规启示

在视频监控场景中，应当遵守数据最小化原则，在充分、相关且必要范围内设置监控范围和时间。

※ 场景化红线

在视频监控场景中，禁止将监控范围扩大到不必要的范围，禁止超出必要范围收集个人数据。

35 HM医院未经授权处理个人数据

※ 处罚金额

48,000 欧元

※ 处罚依据

GDPR 第 5（1）（a）条，第 6 条

※ 处罚时间

2020/2/25

※ 案件事实概述

数据主体投诉表示，在他入院时，他必须填写一个带有复选框的表格，表明数据主体默认同意将他的数据传输给第三方保险公司。每位去急诊室的病人都被告知其住宿费用将按照此方式通知保险公司用于检查保险状态，如果拒绝此类传输，则需要支付相关费用。

※ 违规分析

有效的同意应当满足清晰明确的要求，必须通过声明或明确的肯定性行动（即明示同意方式）作出明确的指示。HM 采取默认同意的方式，要求数据主体默认同意将数据转移给第三方，违反了 GDPR 关于同意应当符合清晰明确的要求。

※ 合规启示

有效的同意应当满足清晰明确的要求，必须通过声明或明确的肯定性行动（即明示同意方式）作出明确的指示。常见的明示同意方式有：a) 主动勾选、点击、滑动、发送等动作；b) 主动填写、输入个人信息；c) 主动开启 API、权限；d) 纸质或电子的书面声明、签字确认；e) 电子签名；f) 电话录音、视频录像等方式。

※ 场景化红线

禁止以默示同意方式要求数据主体同意对其个人数据的处理行为。

36 西班牙沃达丰非法处理儿童个人数据

※ 处罚金额

120,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/2/27

※ 案件事实概述

AAA 先生自己错误地以其儿子的名义在沃达丰线上商店申请了通话服务，在认识到自己的错误后立即联系西班牙沃达丰要求取消该服务，但西班牙沃达丰避重就轻，没有正面回应客户的取消订阅要求，而是问 AAA 先生是否同意将支付方式由后付改为预付，AAA 先生同意，随后收到了西班牙沃达丰邮寄的 SIM 卡；后来由于 AAA 先生未付款，西班牙沃达丰向 AAA 先生的儿子发送信件通知其构成违约，并要求其在收到该通知起 10 日内付清欠款，否则会将其纳入失信名单。但事实上还未到截至日期，仅过了 4 天就将 AAA 先生的儿子列入 ASNEF 档案（类似于失信人档案）。

※ 违规分析

1. 西班牙沃达丰未经数据主体同意处理儿童个人数据；

2. 未能响应数据主体取消服务订阅的请求，而是诱导客户继续履行合同，以不合法、不公正的方式进行处理；

3. 非法将收集的个人数据披露给了信用评价机构；

4. 无法向数据保护监管机构（AEPD）证明数据主体已同意其处理个人数据用来提供电信通话服务。

※ 合规启示

1. 企业在进行数据处理前务必要确保具备相应的合法性基础；

2. 在收到数据主体（包括但不限于客户、用户、员工）注销账户、取消订阅服务等请求后，应及时响应数据主体行权请求并进行相应处理，充分保障数据主体权利；

3. 数据披露、共享、公开应当合法。

※ 场景化红线

1. 企业应严格遵循数据处理的合法性原则，严禁在缺乏合法性基础的前提下处理个人数据；

2. 严禁违规干涉数据主体行权请求及响应处理，也不得不合理地拖延；

3. 严格限制数据披露与共享。

37 AEMA未经授权披露个人数据

※ 处罚金额

3,600 欧元

※ 处罚依据

GDPR 第 5（1）（f）条

※ 处罚时间

2020/2/28

※ 案件事实概述

AEMA Hispánica 公司将一名雇员的工资单寄给另一名雇员，向未经许可的当事人披露了个人数据。该违规行为是出于过失，但事发后负责数据处理的人员未采取任何已知措施减轻相关方的损失，该公司在最终处罚决定下达前未与监管机构进行任何合作以纠正违规并减轻违规可能造成的不利影响。

※ 违规分析

该公司未采取适当的安全保障措施，未核对工资单发送对象和数据主体身份一致性，因此向未经许可的当事人披露了个人数据，违反了数据完整性和保密性原则。在和监管机构的沟通交流过程中，该公司未与监管机构进行任何合作以降低不利影响。

※ 合规启示

1. 在发送工资单前，应将发送对象与数据主体身份进行核对，确认无误后再发送；

2. 发生数据违规事件后，应及时采取适当措施减轻事件带来的损害后果；

3. 在监管机构调查事件中，应与监管机构保持良好的合作关系，积极纠正违规行为并减轻违规可能造成的不利影响。

※ 场景化红线

1. 在财务薪资报酬场景中，禁止未经核查发送对象身份就发送工资单；

2. 在发生数据违规事件后，禁止拒绝与监管机构进行合作以降低不利影响。

38 西班牙沃达丰违反数据安全保障义务

※ 处罚金额

48,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 处罚时间

2020/2/28

※ 案件事实概述

索赔人使用他母亲的账户和密码访问客户区取消以母亲的名义签订的服务时，发现还能访问到其他人的数据。调查发现，系统会向每个用户提供一个代码，以便他们可以查看其发票。出现问题的原因可能在于代理可能会错误地提供相同的代码，这可能会激发获取错误的信息。

※ 违规分析

该公司未能有效评估使用的代码代理系统的安全性和可靠性，未采取合理的技术和组织措施确保数据安全，存在向不同数据主体提供同一安全访问密钥致的可能性，导致个人数据存在泄漏风险，违反了数据安全保障义务。

※ 合规启示

使用计算机系统，应有效评估使用的代码代理系统的安全性和可靠性，并采取合理的技术和组织措施确保数据安全。

※ 场景化红线

对于计算机系统，禁止在未经评估系统安全性和可靠性的情况下直接投入使用。

39 某企业网站缺失隐私政策及Cookies设置

※ 处罚金额

1,800 欧元

※ 处罚依据

GDPR 第 13 条

※ 处罚时间

2020/3/3

※ 案件事实概述

Solo Embrague 网站的主页上没有显示隐私政策或 Cookie 横幅，数据主体无从得知自己被收集的个人数据如何进行处理。

※ 违规分析

根据透明度原则，企业应当将有关数据处理的信息以简洁明了、清晰易懂的形式提供给数据主体，而该公司网站上既没有公示隐私政策，也没有设置 Cookies 横幅，违反了数据处理的透明度原则。

※ 合规启示

1. 企业隐私政策应予以公开、易于访问且清晰易懂，并且包含法律所要求提供的信息；

2. 企业门户网站和运维的其他网站设置 Cookies 应当符合透明度原则。

※ 场景化红线

1. 网站上不得缺失隐私政策及 Cookies 设置；

2. 在隐私声明中不得隐瞒或不充分说明控制者或处理者身份等信息。

40 西班牙沃达丰客户数据泄露事件

※ 处罚金额

42,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条，第 32 条

※ 处罚时间

2020/3/3

※ 案件事实概述

西班牙沃达丰未能证明其采取了足够的技术和组织措施来确保数据安全，导致客户的个人数据遭受了未经授权的访问。

※ 违规分析

根据完整性和保密性原则，企业应当采取适当的技术和组织措施确保数据安全，而西班牙沃达丰未能遵守该原则，导致了个人数据遭受未经授权的访问。

※ 合规启示

企业应采取适当的措施确保个人数据安全，包括采取适的技术和组织措施，以保护数据免遭未经授权的访问或非法处理。

※ 场景化红线

禁止缺失数据安全保障措施。

41 西班牙沃达丰未经同意处理客户个人数据

※ 处罚金额

40,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/3/3

※ 案件事实概述

西班牙沃达丰向数据主体发送了短信，确认该号码与沃达丰签订了电话服务合同，尽管该数据主体并非沃达丰客户。经查，该电话服务合同签约主体的姓名、电子邮件、地址等数据与数据主体不一致，仅注册手机号码是数据主体的。

※ 违规分析

数据处理应当具备合法性基础，西班牙沃达丰未经数据主体授权同意也没有其他合法性基础处理客户个人数据，违反了数据处理的合法性原则。

※ 合规启示

企业在进行数据处理前务必要确保具备相应的合法性基础。

※ 场景化红线

严禁在缺乏合法性基础或法律依据不足情况下处理个人数据。

42 西班牙沃达丰未经授权处理个人数据

※ 处罚金额

24,000 欧元

※ 处罚依据

GDPR 第 5 条、第 6 条

※ 处罚时间

2020/3/4

※ 案件事实概述

该公司向客户发送了两封短信，告知其变更服务合同的费率，并对购买新的移动电话的行为进行确认。但是该客户从未要求改变费率以及购买新电话。

※ 违规分析

该公司数据处理没有合法性基础，未经数据主体同意且不符合其他合法利益。

※ 合规启示

数据处理应合法，选择和适用恰当的合法性基础。通常而言，订立服务或买卖合同应当事先取得数据主体的同意。

※ 场景化红线

在提供服务或产品时，禁止在无数据处理合法性基础的情况下处理个人数据，禁止以数据主体的名义购买服务或产品。

43 私人违规安装使用监控摄像头

※ 处罚金额

4,000 欧元

※ 处罚依据

GDPR 第 5 条

※ 处罚时间

2020/3/6

※ 案件事实概述

行为人违规使用视频监控摄像头，视频监控的覆盖范围超出私人区域，包括了部分公共空间。

※ 违规分析

私人出于维护个人、家庭财产及人身安全等一般目的安装监控摄像头，监控范围应仅限于以上目的，不得超出必要限度侵犯他人高度个人化的生活领域，但违规行为人监控范围包括了部分公共空间，违反了数据最小化原则。

※ 合规启示

1. 企业应谨慎使用视频监控，安装、使用视频监控系统应具备相应合法性基础；

2. 使用视频监控应当符合最小必要原则，摄像头拍摄范围应仅限于安装目的，不得超目的范围拍摄画面。

※ 场景化红线

严禁违规安装、使用视频监控系统。

44 某零售商未充分履行信息告知义务

※ 处罚金额

3,200 欧元

※ 处罚依据

GDPR 第 13 条，第 14 条

※ 处罚时间

2020/3/6

※ 案件事实概述

该零售商使用视频监控系统而未做足够的声明，没有在明显的位置告知摄像头的使用——没有设置明显的的标识，告知进入该区域的人“您已进入视频监控范围”；也没有告知视频监控使用目的、数据主体权利、数据存储位置、期限及采取的安全措施等信息。

※ 违规分析

使用视频监控系统应当遵循 GDPR 第 13 条、第 14 条规定充分履行告知义务。而该零售商并未履行该项告知义务，违反了透明度原则。

※ 合规启示

安装、使用视频监控遵照 GDPR 第 13、14 条的规定充分履行信息告知义务，提供法律所要求提供的信息。基于透明度原则，首先应当在明显的位置告知摄像头的使用，例如在视频监控的区域内应设置明显的的标识，告知进入该区域的人“您已进入视频监控范围”；还应当告知视频监控使用目的、数据主体权利、数据存储位置、期限及采取的安全措施等信息。

※ 场景化红线

严禁违规安装、使用视频监控系统。

45 某酒店非法公开个人数据

※ 处罚金额

15,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条

※ 处罚时间

2020/3/9

※ 案件事实概述

该数据主体声称，他曾向该酒店管理层和工会代表发出一封私人信件，其中载有他所遭受的骚扰事件的信息，并描述了具体的医疗状况。酒店管理层和工会代表随后在与其他雇员的一次会

议上阅读了这封信的内容。

※ 违规分析

医疗健康数据属于敏感个人数据，GDPR 予以特殊保护。包含个人数据的信件本应仅由有处理权限的人员阅读，而该酒店向与会人员公开包含医疗健康数据在内的信件，缺乏适当的组织措施以确保个人数据安全，违反了完整性和保密性原则。

※ 合规启示

企业应采取适当的措施确保个人数据安全，包括采取适的技术和组织措施，以保护数据免遭未经授权或非法处理。

※ 场景化红线

禁止缺失数据安全保障措施。

46 业主协会违规安装使用监控摄像头

※ 处罚金额

2,000 欧元

※ 处罚依据

GDPR 第 5 条，第 13 条，第 14 条

※ 处罚时间

2020/3/12

※ 案件事实概述

该业主协会未经业主的授权在公共区域安装监控摄像头，拍摄范围包括社区内所有的楼梯、走廊，记录所有经过的人。也没有在视频监控的区域内设置明显的标识，告知进入该区域的人“您已进入视频监控范围”；也没有告知视频监控使用目的、数据主体权利、数据存储位置、期限及采取的安全措施等信息。

※ 违规分析

1. 该业主协会未经业主授权安装监控摄像头，首先违反了合法性原则；

2. 数据收集和处理应仅限于数据处理目的最小必要范围，监控公共空间，违反了数据最小化原则；

3. 使用视频监控系统应当遵循 GDPR 第 13 条、第 14 条规定充分履行告知义务。而该业主协会并未履行该项告知义务，这在一定程度上违反了透明度原则。

※ 合规启示

1. 企业应谨慎使用视频监控，安装、使用视频监控系统应具备相应合法性基础；

2. 使用视频监控应当符合最小必要原则，摄像头拍摄范围应仅限于安装目的，不得超目的范围拍摄画像；

3. 安装、使用视频监控遵照 GDPR 第 13、14 条的规定充分履行信息告知义务，提供法律所要求的信息。

※ 场景化红线

严禁违规安装、使用视频监控系统。

47 某企业未经数据主体同意向第三方发送个人数据

※ 处罚金额

5,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条

※ 处罚时间

2020/3/16

※ 案件事实概述

未经数据主体知情同意，Centro De Estudio Dirigidos Delta, S.L. 通过 WhatsApp（Facebook 公司的旗下一款用于智能手机的跨平台加密即时通信应用程序）向第三方发送了三名数据主体（一位母亲及其两个孩子，年龄未知，但可能是未成年人）的姓名和身份证号码等个人数据。

※ 违规分析

数据控制者应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的处理以及意外的丢失、销毁或破坏，Centro De Estudio Dirigidos Delta, S.L. 未经数据主体同意通过第三方软件向其他第三方发送数据主体的个人数据，直接违反了 GDPR 第 5（1）（f）条规定的完整性和保密性原则。

※ 合规启示

1. 企业在进行数据处理前务必要确保具备相应的合法性基础；

2. 数据与第三方共享应当合法并采取相应的安全保障措施。

※ 场景化红线

1. 严禁在缺乏合法性基础或法律依据不足情况下处理个人数据；

2. 严禁非法披露、公开、共享个人数据。

48 某餐厅违规安装使用监控摄像头

※ 处罚金额

6,000 欧元

※ 处罚依据

GDPR 第 5 条，第 13 条，第 14 条

※ 处罚时间

2020/3/16

※ 案件事实概述

该餐厅在 2019 年 5 月至 10 月期间在酒吧露台上安装了八个视频监控摄像头，监控范围涉及公共空间，并将捕获的视频传输至网络，监控公共空间而没有在明显的位置告知摄像头的使用。没有在视频监控的区域内设置明显的的标识，告知进入该区域的人“您已进入视频监控范围”；也没有告知视频监控使用目的、数据主体权利、数据存储位置、期限及采取的安全措施等信息。

※ 违规分析

1. 数据收集和处理应仅限于数据处理目的最小必要范围，该餐厅可以基于维护经营财产和安全安装监控摄像头，但应仅限于经营空间范围，而不应监控公共空间，这直接违反了数据最小化原则；

2. 使用视频监控系统应当遵循 GDPR 第 13 条、第 14 条规定充分履行告知义务。而该餐厅并未履行该项告知义务，这在一定程度上违反了透明度原则。

※ 合规启示

1. 企业应谨慎使用视频监控，安装、使用视频监控系统应具备相应合法性基础；

2. 使用视频监控应当符合最小必要原则，摄像头拍摄范围应仅限于安装目的，不得超目的范围拍摄画像；

3. 安装、使用视频监控遵照 GDPR 第 13、14 条的规定充分履行信息告知义务，提供法律所要求的信息。

※ 场景化红线

严禁违规安装、使用视频监控系统。

49 西班牙电信(Telefónica)不配合监管机构调查

※ 处罚金额

30,000 欧元

※ 处罚依据

GDPR 第 58 条

※ 处罚时间

2020/3/18

※ 案件事实概述

数据主体向电信运营商 Telefónica 请求行使数据访问权和删除权，Telefonica 未能及时响应，数据主体向 AEPD 进行投诉，AEPD 向电信运营商 Telefónica 发布第 TD/00127/2019 号决定，该决定要求 Telefónica 响应数据主体权利请求。

但 Telefónica 未提供所要求的个人数据及信息。

※ 违规分析

1. 数据控制者有义务配合监管机构的调查，在 AEPD 依照 GDPR 第 58 条第 1 款 (a) 项命令数据控制者提供其履行职责所需的个人数据及信息时，Telefónica 没有及时履行义务配合监管机构的调查；

2. 在收到数据主体行权请求后，Telefónica 不合理地拖延、忽视行权请求。

※ 合规启示

1. 企业面对监管部门调查时应当积极配合，与监管机构保持密切、顺畅的沟通；

2. 在收到数据主体行权请求后，应及时响应并进行相应处理，充分保障数据主体权利。

※ 场景化红线

1. 严禁阻挠监管机构调查、拒不配合等行为；

2. 严禁无视、不合理地拖延数据主体行权响应。

50 Xfera Moviles S.A.不配合监管机构调查

※ 处罚金额

5,000 欧元

※ 处罚依据

GDPR 第 58 条

※ 处罚时间

2020/3/25

※ 案件事实概述

数据主体向 Xfera Moviles S.A. 提出了访问其个人数据的请求，Xfera Moviles S.A. 未能及时响应，数据主体向 AEPD 进行投诉。AEPD 要求 Xfera Moviles S.A. 提供其执行任务所需的所有个人数据及信息，但 Xfera Moviles S.A. 没有及时向 AEPD 提供所要求的信息。

※ 违规分析

1. 数据控制者有义务配合监管机构的调查，在 AEPD 依照 GDPR 第 58 条第 1 款 (a) 项命令数据控制者提供其履行职责所需的个人数据及信息时，Xfera Moviles S.A. 没有及时履行义务配合监管机构的调查；

2. 在收到数据主体行权请求后，Xfera Moviles S.A. 不合理地拖延、忽视行权请求。

※ 合规启示

1. 企业面对监管部门调查时应当积极配合，与监管机构保持密切、顺畅的沟通；

2. 在收到数据主体行权请求后，应及时响应并进行相应处理，充分保障数据主体权利。

※ 场景化红线

1. 严禁阻挠监管机构调查、拒不配合等行为；

2. 严禁无视、不合理地拖延数据主体行权响应。

7 德国

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

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

GDPR 第 15 条，第 17 条，第 21 条

※ 处罚时间

2019/8

※ 案件事实概述

有十名该公司前客户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其账号。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。

※ 场景化红线

禁止忽视、延迟响应数据主体的权利请求。

02 某食品公司缺乏对数据安全的保障

※ 处罚金额

100,000 欧元

※ 处罚依据

GDPR 第 5 条，第 32 条

※ 处罚时间

2019/10/24

※ 案件事实概述

该公司在其网站上设立了一个申请门户，有关各方可以在线提交申请文件。但是，该公司没有提供数据的加密传输，也没有以加密或密码保护的方式存储申请人数据。此外，该数据可以链接到 Google，在 Google 上搜索相应申请人姓名的任何人都可以找到他们的申请文件，并在不受访问限制的情况下检索这些文件。

※ 违规分析

该企业未采用加密等安全措施保障数据的安全，并导致数据被非授权访问，违反了 GDPR 第 5 条第 1 款（f）规定的完整性和保密性原则以及第 32 条规定的处理安全。

※ 合规启示

企业应对数据的存储和传输采取加密等安全保障措施，防止任何非授权访问。

※ 场景化红线

禁止不加密进行个人数据的存储和传输。

03 Deutsche Wohnen SE未遵守存储限制原则

※ 处罚金额

14,500,000 欧元

※ 处罚依据

GDPR 第 5 条，第 25 条

※ 处罚时间

2019/10/30

※ 案件事实概述

该公司使用了一个存档系统来存储租户的个人数据，该系统没有提供删除不再需要的数据的可能性。租户的个人数据是在没有检查是否允许或甚至必要的情况下存储的。因此，这些租户的个人数据存储多年，并且仍未用于原始收集的目的。数据类型包括关于租户个人和财务状况的数据，如薪资表、自我披露表、就业和培训合同摘录、税收、社会保障和医疗保险数据以及银行报表。

※ 违规分析

该企业使用无法满足存储限制原则要求的存档系统违反 GDPR 第 5 条第 1 款（e）及 GDPR 第 25 条。此外存储租户的个人数据没有检查是否具备存储此类数据的合法性基础，违反了 GDPR 第 5 条第 1 款（a）的规定。

※ 合规启示

对于非直接从数据主体处获得的个人数据应先检查是否具备处理的合法性基础然后按照 GDPR 第 5 条规定的其他原则进行处理，并且应实施相应的技术和组织措施以确保在默认情形下被处理的个人数据对每个特定处理目的都是必要的。

※ 场景化红线

禁止无限期存储个人数据。

04 某医院混淆数据主体

※ 处罚金额

105,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 处罚时间

2019/12/3

※ 案件事实概述

病人入院时发生了几次与其他病人的混淆，导致计费不正确，并揭示了医院病人管理中的技术和组织结构性缺陷。

※ 违规分析

与其他病人的混淆造成了健康信息这样的特殊类型个人数据的非授权披露，违反了 GDPR 第 32 条处理安全的规定。

※ 合规启示

企业应采取适当的技术和组织措施保障数据主体的个人数据安全，防止数据非授权披露。

※ 场景化红线

禁止将个人数据发送给错误的数据主体。

05 Rapidata GmbH未任命数据保护官

※ 处罚金额

10,000 欧元

※ 处罚依据

GDPR 第 37 条

※ 处罚时间

2019/12/9

※ 案件事实概述

尽管监管机构一再提出要求，电信服务提供商 Rapidata GmbH 并未采取进一步程序按照 GDPR 第 37 条规定的法律要求来任命公司数据保护官。考虑到这是一家微型企业类别的公司，罚款金额为 10,000 欧元。

※ 违规分析

该公司作为一家电信供应商，属于 GDPR 第 37 条第 1 款（b）“核心业务由数据处理组成，该处理因其自身的性质、范围和 / 或目的等需要对数据主体进行定期的、系统化的大规模监控“所指的应当任命数据保护官的情形。不任命的行为违反了 GDPR 第 37 条的规定。

※ 合规启示

企业应根据 GDPR 第 37 条规定的应当任命数据保护官的情形来识别其是否有任命义务。

※ 场景化红线

禁止错误识别和忽略数据保护官任命义务。

06 1&1 Telecom GmbH未采用高安保系数的身份验证

※ 处罚金额

9,550,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 处罚时间

2019/12/9

※ 案件事实概述

1 & 1 Telecom GmbH 是一家提供电信服务的公司。呼叫者只要输入个人客户的姓名和出生日期，就可以从公司的客户服务部门获得有关该个人客户数据的大量信息。在 BfDI 批评其数据保护工作不足后，1 & 1 Telecom GmbH 表现出了自己的洞察力和高度合作。第一步，首先通过查询其他信息来保护身份验证过程。第二步，与 BfDI 协商引入一种新的认证程序，该程序在技术和数据保护方面得到了显着改善。由于该公司与数据保护机构展开积极的合作并及时进行改进，被判处的罚款处于下限。 ※ 违规分析

该公司没有采取足够的技术和组织措施来防止未经授权的人员通过电话从客户服务认证程序中获取有关其客户数据的信息。BfDI 认为此身份验证程序违反了 GDPR 第 32 条，公司没有采取适当的技术和组织措施来系统地保护个人数据的处理。

※ 合规启示

对于验证身份后提供相关个人信息服务的场景，企业应注意采取适当的技术和组织措施提高验证程序的安全性和可信度。

※ 场景化红线

禁止采用安全系数低的身份验证程序。

8 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

150,000 欧元

※ 处罚依据

GDPR 第 5（1）（a）（b）（c）条，第 5（2）条，第 6（1），第 13（1）（c），第 14（1）（c）条

※ 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。

※ 场景化红线

禁止处理员工个人数据时使用不恰当的合法性基础；

禁止不向员工提供 GDPR 要求提供的有关数据处理的信息；

禁止对数据处理行为不进行记录和文档保存。

02 希腊电信公司OTE的电话营销未遵守数据处理原则

※ 处罚金额

400,000 欧元

※ 处罚依据

GDPR 第 5（1）（d）条，GDPR 第 21（3）条，第 25 条

※ 处罚时间

2019/10/7

※ 案件事实概述

该公司由于技术操作上的失误，使得其内部系统中存储的可以用作广告推送的客户信息与提供供应商服务的客户信息发生互联错误。另外，该公司没有适当的措施来响应数据主体“取消订阅”的请求，所以 8,000 名客户的数据没有根据其请求删除。这导致许多客户都受到电话营销的影响，尽管他们已经宣布选择退出。

※ 违规分析

该电信服务公司对其用户个人数据的处理并不准确，相关的客户信息处理发生错误，导致客户受到电话营销的影响，违反了准确性原则；另外，该公司未能设置相应措施实现用户“取消订阅”的请求，违反了关于数据主体拒绝权的相关规定。

※ 合规启示

企业在进行直接营销行为时应当保证使用的个人数据的准确性，避免营销信息发送错误；另外，设置的“取消订阅”机制应保证能够通过相关的技术手段得到落实。

※ 场景化红线

禁止对用户“取消订阅”的请求不予落实。

03 WIND公司的电话营销未充分实现数据主体权利

※ 处罚金额

20,000 欧元

※ 处罚依据

GDPR 第 21 条

※ 处罚时间

2019/10/18

※ 案件事实概述

希腊数据保护监管机构基于收到的 6 份关于 WIND 公司的电话营销投诉，对其展开调查。在调查过程中，了解到 WIND 公司在针对个人进行 WIND 相关产品和服务的推介时，忽视了受影响方针对广告电话提出的异议。用户要求删除电话号码或拒绝其电话号码用于此种广告目的要求未能得到满足。

※ 违规分析

该公司使用用户的个人数据用于营销目的，用户有权随时拒绝为此类营销目的而处理其个人数据的行为。该公司未能实现数据主体的请求，违反了数据主体拒绝权行使的相关的规定。

※ 合规启示

企业在进行直接营销行为时应当设置适当的方式允许受影响的个人随时拒绝这种营销行为，比如一键退订等方式。

※ 场景化红线

禁止在用户拒绝以营销方式使用其个人数据

时仍继续推送营销类信息。

04 爱琴海石油集团未采取必要措施保证数据处理安全

※ 处罚金额

150,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 32 条

※ 处罚时间

2019/12/19

※ 案件事实概述

爱琴海石油集团以外的公司已获得对其包含个人数据的服务器的访问权，并复制了服务器的内容。爱琴海石油公司未能采取必要的技术措施来确保处理服务器中存储的大量数据的安全。此外，爱琴海石油公司并未将相关软件与存储在服务器中的个人数据分开存放，这导致了服务器内容的非法复制。爱琴海石油公司尚未告知数据主体有关服务器中包含的其个人数据的处理情况。

※ 违规分析

该公司未能采取必要的技术措施保护相关个人数据不被非法处理，未能满足数据处理安全性要求，违反了数据处理完整性和保密性原则；另外该公司并未告知数据主体有关服务器中包含其个人数据的处理情况，违反了数据处理合法、公平、透明的要求。

※ 合规启示

1. 企业所使用的服务器设备需要有适当的技术和组织措施保障数据处理的安全，防止不当操作带来数据泄露等违规事件；

2. 企业应当对服务其中的数据进行分级分类，对其中的个人数据应当设置适当的访问处理权限，防止非授权方的访问和拷贝等。

※ 场景化红线

不得对服务器中的数据不作区分地混乱化管理导致数据发生泄露。

05 Allseas Marine处理员工数据未遵守数据处理原则

※ 处罚金额

15,000 欧元

※ 处罚依据

GDPR 第 5（1）（a），（2）条

※ 处罚时间

2020/1/13

※ 案件事实概述

希腊数据保护监管机构针对“ ALLSEAS MARINE S.A.”员工投诉内容进行了调查，调查涉及公司在服务器上处理个人数据的合法性，以及在有合理理由怀疑其高级经理的违法行为损害了公司利益的情况下，访问和检查受到怀疑的人员的电子邮件的合法性。

监管机构发现，公司内部政策和法规规定，禁止员工将公司的电子通信和网络用于私人目的，并有基于此进行内部检查的可能性。因此，公司拥有 GDPR 第 5 条第 1 款和第 6 条第 1 款（f）项的合法利益，可以进行内部调查以检查员工的电子邮件。

另一方面，监管机构发现闭路视频监控系统是非法安装和运行的，此外，提交给监管机构的记录材料也被认为是非法的。

最后，监管机构发现该公司不满足员工访问其公司电脑中包含的其个人数据的权利。

※ 违规分析

该公司对员工数据在工作场所的处理程度及视频监控系统的引入，是非法的，这违反了数据处理的合法性原则；公司没有向员工充分通报数据处理的相关信息，违反数据处理的公平透明原

则；该公司向监管机构提供相关材料不能证明其对相关原则的落实情况，违反了责任原则。

※ 合规启示

1. 企业在安装使用视频监控设备时，应充分考虑数据处理的合法性基础，一般以合法利益作为数据处理的合法性基础的情况下，要保证企业相关合法利益高于数据主体的合法利益；

2. 视频监控设备的安装要注意对数据主体履行充分性告知义务，使数据主体能够了解到视频监控行为存在的事实，同时提供适当途径使数据主体有机会了解到数据处理有关的更全面的信息。

※ 场景化红线

不得在员工办公场所对其进行持续性、永久性的监控。

06 公共电力公司未充分实现数据主体权利

※ 处罚金额

5,000 欧元

※ 处罚依据

GDPR 第 15 条

※ 处罚时间

2020/2/21

※ 案件事实概述

申诉人要求获得 2015 年至今与该公共电力公司之间进行物理和电子通信内容的副本。该公共电力公司作为数据控制者，在收到其用户访问请求后的一个月内未予回复，未能通知数据主体其无法满足访问权的事实。

※ 违规分析

申诉人提出的获取其个人数据处理的内容副本的请求属于行使访问权的范畴，该公共电力公司作为数据控制者，未能在规定时间内答复数据主体的访问权请求，违反了关于数据主体访问权的相关规定。

※ 合规启示

1. 数据主体有权获得对其个人数据处理的相关内容，而且企业作为数据控制者还必须向其提供所处理的个人数据的副本，对此，数据主体不需要说明申请的理由；

2. 企业在收到数据主体的访问权等权利请求时，需要在一个月内予以回复，考虑到请求的复杂性等，在必要时可再延长两个月，但需要在收到请求起一个月内将延期情况和原因及时告知。

※ 场景化红线

不得要求数据主体提供其行使相关权利的动机和原因；

不得对数据主体的行权请求无故拖延。

07 Mihou Dimitra未充分实现数据主体权利

※ 处罚金额

8,000 欧元

※ 处罚依据

GDPR 第 15 条，第 58 条

※ 处罚时间

2020/3/20

※ 案件事实概述

申诉人要求获得其子女的数据和税务资料。此请求被数据控制者拒绝。此外，在数据保护监管机构下发调查命令时，要求数据控制者提供其履行义务相关的必要信息时，数据控制者未能满足。为此，两项违规行为共处以 8000 欧元的罚款，其中 3000 欧元因未响应数据主体的访问权，另外 5000 欧元因违反数据保护监管机构的命令。

※ 违规分析

该培训机构处理未成年人个人数据，其监护人有权对个人数据进行访问，培训机构未能满足相关权利请求，违反了数据主体访问权的相关规定；该培训机构作为数据控制者，应当在监管机

构对其进行调查时，提供信息证明其义务履行的充分性，由于未能提供必要信息，违反了责任原则。

※ 合规启示

1. 企业处理个人数据时，应当设置适当的流程机制保障数据主体权利的实现；

2. 企业处理的个人数据中涉及儿童个人数据的处理时，首先应获得其监护人的同意，同时应允许其监护人行使数据主体的各项权利；

3. 企业应当能够证明其自身履行数据保护相关义务的情况，能够在涉及监管机构调查时，提供充分的证明材料。

※ 场景化红线

禁止忽视或瞒报数据主体的行权请求；

禁止忽视、不配合、阻碍数据保护监管机构行使调查权。

9 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

130,000 欧元

※ 处罚依据

GDPR 第 5（1）（c）条，第 25（1）条

※ 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，在内外部交易中泄露了 337,042 个数据主体的身份信息和地址。

※ 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。

※ 场景化红线

禁止对数据处理采取不充分的技术组织措施。

02 WORLD TRADE CENTER数据泄露事件

※ 处罚金额

15,056 欧元

※ 处罚依据

GDPR 第 32 条

※ 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。

※ 场景化红线

禁止通过拍摄等手段将个人数据进行未经授权的发布和传播。

03 LEGAL COMPANY & TAX HUB SRL数据泄露事件

※ 处罚金额

3,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 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。

※ 场景化红线

禁止对网站中处理的个人数据采取安全性较低的保障措施。

04 某公司运营的网站个人数据处理的法律依据不足

※ 处罚金额

9,000 欧元

※ 处罚依据

GDPR 第 5（1）（a）条，第 6（1）（a）条

※ 处罚时间

2019/9/26

※ 案件事实概述

Webseitavocatnet.ro 网站注册过程中使用了一个未勾选的复选框，用户只有勾选该复选框，才表示用户不希望通过电子邮件接收相关信息（选择退出 opt-out）。在没有任何操作的情况下，会自动通过电子邮件向用户发送相关信息。该行为涉及了 4,357 个用户。

※ 违规分析

对于该网站的用户来说，只要用户忽略了此复选框，就会自动订阅，或者将他的电子邮件自动输入到用户库中以获取相关信息。因此，订阅是在用户没有明确意愿表达的情况下进行的。该网站运营商基于其所要进行的数据处理未能获得有效的同意，违反了数据处理合法性要求。

※ 合规启示

企业处理个人数据若需要获得数据主体的同意，则同意应当在数据处理之前作出，并需要通

过清楚明确的行为自愿表明同意对其个人数据的处理。同意的方式可以包括在浏览网页时在方框中打钩以清楚表示接受对其个人数据的处理，而默示、预选方框或者不作为不构成同意。

※ 场景化红线

禁止在网页中通过用户默示同意的方式处理个人数据。

05 Raiffeisen银行与Vreau Credit公司数据泄露事件

Raiffeisen Bank SA

※ 处罚金额

150,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 处罚时间

2019/10/9

Vreau Credit SRL

※ 处罚金额

20,000 欧元

※ 处罚依据

GDPR 第 32 条，第 33 条

※ 处罚时间

2019/10/9

※ 案件事实概述

这起调查针对的是两家公司的联合行为。Raiffeisen 银行的两名员工从 Vreau 信贷公司的两名员工处，通过 Whatsup 应用程序，获得了 Vreau 信贷平台中注册的用户的个人数据。同时将所获得的个人数据上传到国家信贷征信系统中进行分析处理，通过计分模拟，获得必要的数据以便确定个人的信用资格。累计对 1177 个人进行了 1194 次仿真处理。对于其中 124 个人，还查询了 ANAF 数据库（罗马尼亚国家财政行政局的数据库）。同时 Raiffeisen 银行的员工将否定的贷款决定传达给 Vreau Credit SRL 员工。另外，对于从 Vreau 信贷公司，直到此次调查结束前，也没有将相关数据泄露事件通知到监管机构。

※ 违规分析

该银行没有采取适当的措施来确保处理数据的员工在其授权下行事，也没有采取适当的技术和组织措施来确保适当的安全级别，导致在信贷活动中该银行的员工通过应用程序对个人数据进行了非授权的处理和披露。

该信贷平台公司直到本次调查结束，亦未向监管机构通知数据泄露事件的发生，尽管该公司早在 2018 年 11 月就已经发现该数据泄漏事件。该公司的行为违反了向监管机构报告个人数据泄露的义务，数据控制者有义务自发现数据泄露事件之时起 72 小时内通知数据监管机构。

※ 合规启示

1. 企业对所处理的个人数据进行授权管理时，应当采取适当的措施保证被授权的个人按照其指示行事，防止进行非法数据处理，可采取的措施比如通过签署授权范围明确的授权函等；

2. 企业应当设置有效的数据泄露响应流程机制，确保数据泄露通知义务的履行，比如在发现数据泄露事件的之时起，72 小时内通知监管机构的义务。

※ 场景化红线

禁止将个人数据披露给非授权第三方；

禁止忽视或瞒报数据泄露事件。

06 某公司安装视频监控设备未履行充分性告知义务

※ 处罚金额

2,500 欧元

※ 处罚依据

GDPR 第 12 条，第 13 条，第 5（1）（c）条，第 6 条

※ 处罚时间

2019/10/17

※ 案件事实概述

该公司无法证明安装视频监控系统对个人数据（图像）进行处理履行了充分性告知义务，且自 2016 年以来，这些视频监控设备一直在运作；另外，公司在公开的通知栏上披露了 2018 年 ISCIR（罗马尼亚某国家机构）授权人员的培训报告，从而披露了员工的相关个人数据，并且无法证明数据处理的合法性。

※ 违规分析

该公司安装视频监控系统未向受到监控影响的人员（员工）履行充分性告知义务，违反了 GDPR 关于数据控制者从数据主体处收集个人数据时应提供信息的义务；另外，该公司披露了员工的数据却无相关合法性基础，违反了数据处理的合法性要求。

※ 合规启示

1. 企业在安装视频监控设备时，有义务通过清晰易懂、简洁明了、透明以及易获得的方式将有关数据处理的信息提供给数据主体。

2. 企业在披露相关文件时，对于其中涉及的个人数据的披露应当尽量避免或做好匿名化，如果一定要披露，需要有相关合法性基础。

※ 场景化红线

禁止在安装视频监控设备时不满足充分性告知的义务；

禁止在无相关合法性基础的情况下公开披露个人数据。

07 个人理财公司未满足数据主体权利的实现

※ 处罚金额

2,000 欧元

※ 处罚依据

GDPR 第 12 条，第 17 条

※ 处罚时间

2019/11/22

※ 案件事实概述

该个人理财公司在收到某客户自然人的删除请求时，没有在 GDPR 规定的期限内（一个月内）做出回应，无故拖延响应数据主体的请求。

※ 违规分析

该公司作为数据控制者在收到数据主体行使删除权的请求时，无特殊延长理由在一个月内未予响应，违反了 GDPR 对数据主体权利相关的规定。

※ 合规启示

企业处理个人数据时，应当设置适当的流程机制保障数据主体权利的实现。

※ 场景化红线

禁止忽视或瞒报数据主体的行权请求。

08 快递服务公司因技术组织措施不足造成数据泄露

※ 处罚金额

11,000 欧元

※ 处罚依据

GDPR 第 5 条（1）（f），第 32 条

※ 处罚时间

2019/11/25

※ 案件事实概述

该快递服务公司未能采取适当的技术和组织措施，导致约 1100 个数据主体的个人数据（姓名、银行卡号、安全卡代码（CVV）、持卡人地址、个人识别号、序列号和身份证号码、银行账户号、授权信贷限额）丢失和未经授权访问。

※ 违规分析

该快递公司因未设置有效的技术和组织措施，使得大量的个人数据发生丢失和未经授权的访问和泄露，违反了数据处理安全性的要求。

※ 合规启示

企业涉及快递服务，一般会涉及收、发件人较多个人数据的处理，对此应当采取适当的技术组织措施保证所处理的个人数据的安全，防止未经授权的访问。

※ 场景化红线

禁止对个人数据进行未经授权的访问。

09 与数据保护监管机构合作不足四起案件

Modern Barber

※ 处罚金额

3,000 欧元

※ 处罚依据

GDPR 第 58（1）（a）（e）条

※ 处罚时间

2019/11/26

Nicola Medical Team 17 SRL

※ 处罚金额

2,000 欧元

※ 处罚依据

GDPR 第 58（1）（a）（e）条

※ 处罚时间

2019/12/2

Globus Score SRL

※ 处罚金额

2,000 欧元

※ 处罚依据

GDPR 第 58（1）（a）（e）条

※ 处罚时间

2019/12/16

SOS Infertility 协会

※ 处罚金额

2,000 欧元

※ 处罚依据

GDPR 第 58（1）（a）（e）条

※ 处罚时间

2020/3/25

※ 案件事实概述

数据保护监管机构进行调查时要求协会提供更详细的信息，没能及时提供和回应。

※ 违规分析

该协会作为数据控制者未能按照数据保护监管机构的要求提供有关数据处理的信息，违反了数据保护监管机构行使调查权的相关规定。

※ 合规启示

企业在收到数据保护监管机构的调查通知时，应当及时响应配合，否则会因未响应监管机构要求而被处以罚款。

※ 场景化红线

禁止忽视、不配合、阻碍数据保护监管机构行使调查权。

10 ING银行因技术组织措施不足造成重复交易

※ 处罚金额

80,000 欧元

※ 处罚依据

GDPR 第 25 条，第 5 条（1）（f），第 32 条

※ 处罚时间

2019/11/28

※ 案件事实概述

该银行所运营的数据处理系统并未从设计之初就确保遵守数据保护原则，也没有确保其默认

的隐私保护。在影响 225,525 个客户的卡交易结算过程中，该银行没有采取适当的技术和组织措施建立自动数据处理系统，导致 2018 年 10 月 8 日至 10 日期间进行重复交易。

※ 违规分析

该银行违反了关于设计和默认的隐私保护相关的规定，自动化处理个人数据的信息系统因缺乏足够的技术和组织措施导致对数据主体造成影响。

※ 合规启示

企业运营管理的数据处理系统，尤其是涉及自动化数据处理，要关注对系统的设计和默认隐私保护，采取适当的技术和组织措施对自动化系统中能够有效地实施数据保护原则和满足数据主体的权利创造条件 .

※ 场景化红线

不得忽视自动化数据处理系统中的设计及默认隐私保护。

11 某业主协会未履行充分性告知义务及安全保障义务

※ 处罚金额

500 欧元

※ 处罚依据

GDPR 第 12 条，第 13 条，第 25 条，第 32 条

※ 处罚时间

2019/11/29

※ 案件事实概述

该业主协会使用视频监控系统处理图像类个人数据，但没有根据 GDPR 第 13 条向进入该系统的数据主体提供适当的信息，以及没有采取足够的技术和组织安全措施来保护通过视频监视系统收集的个人数据。

※ 违规分析

该业主协会在安装视频监控设备时，未履行对数据主体有关其个人数据处理的充分性告知义务，违反了透明性相关要求；同时没有采取充分的技术组织措施保护所收集的个人数据，违反了数据处理安全性的要求。

※ 合规启示

1. 企业在安装视频监控设备时，有义务通过清晰易懂、简洁明了、透明以及易获得的方式将有关数据处理的信息提供给数据主体。考虑到需要向数据主体提供的信息量，数据控制者可以遵循分层方法，选择使用多种方式组合呈现以确保透明度。关于视频监控，最重要的信息应显示在警告标志本身（第一层）上，而进一步的强制性详细信息可通过其他方式（第二层）提供。

2. 企业应当设置适当技术组织措施，保障视频监控设备处理个人数据的安全性。

※ 场景化红线

禁止在安装视频监控设备时不满足充分性告知的义务，如未张贴警示标志，未提供完整隐私通知书等。

12 Royal President公司未满足数据主体权利的实现

※ 处罚金额

2,500 欧元

※ 处罚依据

GDPR 第 15 条，第 12 条（3）（4），第 5 条（1）（f），第 32 条

※ 处罚时间

2019/11/29

※ 案件事实概述

该公司拒绝了根据 GDPR 第 15 条提出的查阅个人数据的请求，并在未经数据主体同意的情况下披露了个人资料。此外，该公司管理的住宿

卡片没有采取适当的技术或组织措施来确保所处理数据的安全性。

※ 违规分析

该公司未能在规定的期限内满足数据主体行使访问权的请求，违反了数据主体权利响应相关的规定；同时未能采取足够的技术组织措施确保数据不被非法披露，违反了数据处理的完整性和保密性原则。

※ 合规启示

1. 企业应当设置相应的流程机制保证数据主体行权得到恰当有效的响应；

2. 企业应当设置适当技术组织措施，保障数据处理的安全性，防止数据非法泄露。

※ 场景化红线

禁止忽视或瞒报数据主体的行权请求；

禁止将个人数据披露给非授权第三方人员。

13 航空公司未采取充分的安全措施

※ 处罚金额

20,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 处罚时间

2019/12/4

※ 案件事实概述

该航空公司没有采取适当措施确保在其监督下行事的任何自然人按照其指示处理个人数据（GDPR 第 32（4）条）。这导致一名员工未经授权访问预订应用程序，对 22 名乘客 / 客户的个人数据进行拍照，并在互联网上披露此列表。

※ 违规分析

该航空公司未能实施有效的管控措施，导致其客户的个人数据被其员工非法处理并泄露到网上，违反了数据处理的安全性要求。

※ 合规启示

企业应当对其授权处理个人数据的员工进行充分的培训及提示，采取措施保证其按照企业指示处理数据，防止其对个人数据进行违法处理，造成安全泄露事件。

※ 场景化红线

授权处理个人数据的员工不得将其处理的个人数据通过拍照等手段进行非法披露和传播。

14 Hora Credit公司未采取充分的安全措施

※ 处罚金额

14,000 欧元

※ 处罚依据

GDPR 第 5 条，第 25 条，第 32 条，第 33 条

※ 处罚时间

2019/12/10

※ 案件事实概述

该公司将包含他人个人数据的文件传送到错误的电子邮件地址。经调查后发现，该公司处理数据时没有提供有效机制来核实和验证收集的数据的准确性。同时该公司未采取充分的安全保障措施避免未经授权的访问或向第三方披露个人数据。另外，该公司没有在其发现安全事件的 72 小时内将其通知到数据保护监管机构。针对上述三项违法行为，分别处罚 3,000 欧元、10,000 欧元和 1,000 欧元的罚款。

※ 违规分析

该公司未能提供有效的措施核验收集数据的准确性，且缺乏相应的技术组织措施保证数据处理的安全性，导致邮件的错误发送从而泄露了个人数据，违反了数据处理的准确性原则及安全性要求，同时未在 72 小时内通知监管机构，违反了向监管机构报告个人数据泄露的义务。

※ 合规启示

企业应设置适当技术组织措施，避免在对外提供或发送数据时，将个人数据披露给非授权方。同时在发生数据泄露的情形时，该数据泄露可能会对自然人的权利自由造成风险，应当自发现之时起 72 小时内将相关情况报告监管机构。

※ 场景化红线

禁止因技术组织措施不足导致将个人数据披露给非授权第三方人员；

禁止忽视或瞒报数据泄露事件。

15 某公司处理员工个人数据未遵守数据处理原则

※ 处罚金额

10,000 欧元

※ 处罚依据

GDPR 第 5（1）条，第 6 条，第 7 条，第 9 条

※ 处罚时间

2019/12/13

※ 案件事实概述

公司在办公室内及员工存放备用衣服的储物柜（更衣室）中安装摄像头，过度处理了员工的个人数据；另外该公司处理员工的生物特征数据（指纹）用于进入某些房间，实际上公司可以使用对员工个人隐私侵犯较少的方法实现同样的目的。

※ 违规分析

该公司安装视频监控设备处理员工个人数据，以及使用员工的生物特征数据用于门禁系统，超出了数据处理目的的最小范围，违反了最小范围原则。

※ 合规启示

1. 企业在安装视频监控设备时，需要充分考量视频监控设备安装合法性以及其监控范围所处理的数据是否限于数据处理目的的最小必要范围，必要时可以进行数据保护影响评估以评估风险；

2. 企业使用生物特征数据等特殊类型的个人数据时，要尤其关注数据处理的合法性。GDPR 对特殊类型个人数据的处理设置了较严格的限制条件，原则上是禁止处理的，除非有例外情况，比如明确有效地同意。

※ 场景化红线

禁止在员工办公区域安装视频监控设备进行持续性监控；

在有其他对个人隐私侵犯较小的替代方式下，禁止使用特殊类型的个人数据达到相同目的。

16 供电公司数据处理的法律依据不足

※ 处罚金额

6,000 欧元

※ 处罚依据

GDPR 第 5 条（1）（d）（2），第 6 条，第 7 条，第 21（1）条

※ 处罚时间

2019/12/16

※ 案件事实概述

该公司非法处理了一个人的个人数据，无法证明向其邮件发送通知是在当事人同意之后实施的。此外，尽管当事人一再行使拒绝权要求其停止发送，但该公司没有采取必要措施停止发送通知。

※ 违规分析

该公司对该当事人的个人数据处理缺乏适当的合法性基础，同时在当事人行使拒绝权后，不予响应，违反了数据主体拒绝权的相关规定。

※ 合规启示

企业如果要使用同意作为个人数据处理的法律依据，时间上需要在进行数据处理之前获得数据主体的同意，同时需要在数据主体行使相关权利时及时响应。

※ 场景化红线

禁止在未取得相关合法性基础之前处理个人数据。

17 罗马尼亚电信不当披露个人数据

※ 处罚金额

2,000 欧元

※ 处罚依据

GDPR 第 5（1）（d）条，第 32 条

※ 处罚时间

2019/12/18

※ 案件事实概述

该公司未能确保个人数据处理的准确性，导致发送到某一客户住处的发票信息错误发送给另一客户，从而不当披露了个人数据。

※ 违规分析

因技术组织措施不足，该公司对其客户个人数据的处理发生错误，导致数据的非授权披露，违反了数据处理准确性原则和数据处理安全性要求。

※ 合规启示

企业在处理个人数据时，应当确保数据是准确的，且应保持适时更新，采取一切合理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。

※ 场景化红线

禁止因技术组织措施不足导致将个人数据披露给非授权第三方人员。

18 罗马尼亚沃达丰错误处理 个人数据

※ 处罚金额

3,000 欧元

※ 处罚依据

GDPR 第 5（1）（d）（f），（2）条

※ 处罚时间

2020/2/11

※ 案件事实概述

该公司在处理投诉的过程中，处理人员发生失误，将与该投诉相关的内容发送到错误的电子邮件地址。这实际上属于未采取足够的安全措施来防止这种错误的数据处理。

※ 违规分析

因技术组织措施不足，以及相关人员的误操作，使得个人数据发生泄漏，违反了数据处理的完整性和保密性原则。

※ 合规启示

企业应设置适当技术组织措施，避免在对外提供或发送数据时，将个人数据披露给非授权方。

※ 场景化红线

禁止因技术组织措施不足导致将个人数据披露给非授权第三方人员。

19 Enel Energie SA不当披露个人数据

※ 处罚金额

3,000 欧元

※ 处罚依据

GDPR 第 32 条

※ 处罚时间

2020/3/25

※ 案件事实概述

由于该公司未能实施适当的技术和组织措施来确保足够的信息安全水平，该公司向某一自然人客户发送了包含另一个客户个人数据的电子邮件，具体包括姓名、地址、电子邮件地址和客户代码。

※ 违规分析

因技术组织措施不足，该公司将其客户个人数据通过电子邮件的方式发送给其他人，违反了个人数据处理安全方面的要求。

※ 合规启示

企业应设置适当技术组织措施，避免在对外提供或发送数据时，将个人数据披露给非授权方。

※ 场景化红线

禁止因技术组织措施不足导致将个人数据披露给非授权第三方人员。

20 Dante International数据处理的法律依据不足

※ 处罚金额

3,000 欧元

※ 处罚依据

GDPR 第 6 条，第 21（3）条

※ 处罚时间

2020/3/25

※ 案件事实概述

该公司在 2019 年底向客户个人发送了一封商业电子邮件，尽管该数据主体已在 2019 年初取消了对营销信息的订阅。

※ 违规分析

该公司在客户行使拒绝权后，仍向该客户发送营销类信息，违反了关于数据主体对直接营销行使拒绝权的规定。

※ 合规启示

一旦数据主体以取消订阅的方式行使了 GDPR 第 21 条规定的拒绝权，则对未能从商业营销列表中删除数据主体的电子邮件地址而向其发送商业信息的行为，将会被处以罚款。

※ 场景化红线

禁止对用户“取消订阅”的请求不予落实。

10 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 Town of Kerepes选择的合法性基础不恰当

※ 处罚金额

15,100 欧元

※ 处罚依据

GDPR 第 6（1）条

※ 处罚时间

2019/10/1

※ 案件事实概述

该城镇设置的视频监控以其合法利益为数据处理的合法性基础。

※ 违规分析

根据第 6（1）（f）条，公共权力机构执行任务时实施的数据处理不适用合法利益。因此该市选择的合法性基础不恰当，数据处理活动没有法律依据。

※ 合规启示

企业应选取适当的合法性基础作为数据处理的依据。

※ 场景化红线

禁止在不满足合法性基础要求的情况下处理个人数据。

02 某军事医院未充分履行数据泄露通知义务

※ 处罚金额

7,400 欧元

※ 处罚依据

GDPR 第 32 条，第 33 条

※ 处罚时间

2019/10/24

※ 案件事实概述

一家军事医院没有在发现数据泄露事件的 72 小时内报告监管机构，且未能记录与数据泄露有关的事实。作为医院，其处理大量的医疗数据，未能采取有效的技术和组织措施防止数据泄露的发生。

※ 违规分析

没有在规定时间内向监管机构报告数据泄露事件且没有履行数据泄露事件的记录义务。没有采取适当的技术和组织措施防止数据泄露的发生。

※ 合规启示

企业应考虑处理的数据的敏感程度、体量、目的以及实施成本等因素选择适当的技术和组织措施保障数据安全。应在发现数据泄露事件后的规定时间内通知监管机构并履行记录义务。

※ 场景化红线

禁止非法延迟向监管机构报告数据泄露事件。

03 某公司私自检查雇员的通讯设备

※ 处罚金额

2,860 欧元

※ 处罚依据

GDPR 第 5（1）（a），第 6（1）（f）条，第 13 条，第 24 条，第 25 条

※ 处罚时间

2019/10/15

※ 案件事实概述

一名雇员休病假时，其雇主检查了他的台式电脑、笔记本电脑和电子邮件，以确保在其缺勤的情况下他的工作职责的履行，并且该雇主中止了他的帐户。该雇员向监管机构投诉，声称他没有收到事先通知，也没有机会复制和删除他的私人信息（例如：电话号码）。

※ 违规分析

监管机构理解没有履行职责的缺勤雇员可能会带来财务和法律的风险。因此，采取措施预防或减轻这些风险符合雇主的合法商业利益。但是这些措施应当符合数据保护的相关要求。以合法利益作为数据处理的前提是经过必要性测试和平衡测试，该公司未能在具备相应的合法性基础以及告知员工的前提下就进行此类监控活动。

※ 合规启示

监管机构要求：

1. 就业协议必须规定雇员是否可以将工作设备用于私人目的；

2. 隐私通知必须包含员工监控的原因（例如业务连续性、内部调查、纪律目的和员工数据的

特定保留期 -- 包括备份副本的长度）；

3. 雇主还必须进行“平衡测试”，以证明其在一般员工监控和特殊情况下的合法权益。

※ 场景化红线

禁止在缺乏平衡测试的情况下将合法利益作为数据处理的依据。禁止在不告知员工的情况下进行监控行为。

04 某公司未响应数据主体的权利请求

※ 处罚金额

4,440 欧元

※ 处罚依据

GDPR 第 5（1）（a）条，第 17 条

※ 处罚时间

2019/11/11

※ 案件事实概述

某公司基于数据主体的同意处理其电话号码，数据主体请求撤回同意并行使删除权要求删除其电话号码，该公司未遵照数据主体的请求删除相关数据，并继续进行处理。

※ 违规分析

没有响应数据主体的删除权请求，在数据主体撤回同意后已经没有数据处理的合法性基础仍继续处理个人数据。

※ 合规启示

企业应在数据主体撤回同意且没有其他支持个人数据处理的合法性依据时及时删除相关个人数据。

※ 场景化红线

禁止继续处理已撤回同意的个人数据。

05 某公司非法处理前雇员的电子邮件

※ 处罚金额

1,430 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 13 条，第 24 条，第 25 条

※ 处罚时间

2019/12/11

※ 案件事实概述

某公司恢复了一年前离开公司的一位董事的邮箱，发现了一封载有工作相关文件的电子邮件。该前董事向监管机构投诉称他没有收到关于他的前收件箱将被启动的警告，也没有机会复制和删除他的私人信息（例如：密码、财务信息等）。

※ 违规分析

在没有告知、不具备合法性基础的情况下处理包含前雇员个人数据的电子邮件。

※ 合规启示

监管机构要求：

1. 即使雇佣关系已经终止，在查阅该员工的数据时，员工或其代表也应在场；

2. 员工应该能够请求一个数据的副本或删除他们的个人数据；

3. 雇主必须对 IT 资产、电子邮件账户的存档和使用采取内部政策，包括程序规则，如规定检查步骤和授权进行检查的人员。

※ 场景化红线

禁止在未告知或不具备合法性基础的情况下处理前雇员的个人数据。

11 意大利

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

立法概况

● 第 101/2018 号法令《隐私法》(2018 年 9 月 19 日生效)

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

电话：(06 1) 457 7100

传真：(06 1) 356 5520

01 Eni Gas e Luce（Egl）非法处理个人数据

※ 处罚金额

11,500,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 17 条，第 21 条

※ 处罚时间

2019/12/11

※ 案件事实概述

Eni Gas e Luce（Egl）在广告活动和未经请求的合同启动过程中非法处理了个人数据。850 万欧元的第一笔罚款针对的是与电话销售活动有关的非法个人数据处理。除其他违规事项外，该公司未经联系人同意进行电话营销，或尽管该人对此表示拒绝仍进行电话营销，或未进行检查公众退出登记簿的特殊程序而进行电话营销。此外，对用户的个人数据保护缺乏适当的技术和组织措施；处理数据的时间超过了允许的数据保留期；潜在客户的个人数据是从未经同意披露此类数据的实体（列表提供者）中收集的。第二次罚款 300 万欧元涉及因在所谓的“市场经济”条件下未经请求而签订的电力和天然气供应合同而造成的侵权。许多人向监管机构投诉，他们只有在收到与先前供应商的合同终止书或第一张 Eni Gas e Luce（Egl）发票后才得知新合同的签订。在某些情况下，该公司在合同中报告了虚假信息并伪造了签名。

※ 违规分析

该电力及天然气公司无适当合法性依据而进行电话营销活动，且在用户行使拒绝权后仍进行数据处理，违反了数据处理合法性的规定，以及关于满足数据主体拒绝权的规定；数据存储时间超出了允许保留期，违反了存储限制原则；另外未经允许运用系统中的用户信息和用户自动订立供应合同，这里对个人数据的处理违反数据处理合法性的规定。

※ 合规启示

1. 企业在进行营销活动时，涉及个人数据的收集处理需要获得数据主体的同意；

2. 企业在涉及营销活动的数据处理时，针对数据主体的删除权、拒绝权等权利的行使一般不存在豁免条件；

3. 企业从第三方处获得的个人数据，进行处理时应当具备合适的合法性基础，如获取用户的同意等。

※ 场景化红线

未经数据主体有效同意，禁止进行以营销为目的的个人数据处理；

从第三方处获取的个人数据，禁止在无相关合法性基础的情况下进行处理。

02 TIM电信运营商电话营销违反多项数据保护规定

※ 处罚金额

27,800,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 17 条，第 21 条，第 32 条

※ 处罚时间

2020/1/15

※ 案件事实概述

在 2017 年 1 月至 2019 年之间，数据保护监管机构收到了有关该公司的数百份报告和投诉，特别是关于未经数据主体同意的商业推销类电话，或者已在异议登记簿中进行反对登记的主体仍在未经请求下接到相应的电话，或者在数据主体已行使拒绝权的情况下仍然能接到相关电话。此外，公司的应用程序中提供的有关个人数据处理的信息不准确也不透明，并且使用了无效的同意。在某些情况下，关于获取数据主体基于某一处理目的的同意的纸质表格被用于包括营销在内的其他各种目的。此外，数据保存的时间超过了必要的时间，因此违反了存储限制原则。

※ 违规分析

该电信公司对营销活动（电话营销和冷拨电话）未征得数据主体的同意，未能满足数据主体的不以营销目的使用其联系方式的要求，应用程序中收集的同意是无效的，缺乏适当的安全措施保护个人数据（包括与呼叫中心的黑名单交换不正确），缺乏明确的数据保留期限，违反了存储限制原则。

※ 合规启示

1. 企业在进行营销活动时，涉及个人数据的收集处理需要获得数据主体的同意；

2. 企业进行营销活动处理个人数据时，所获得的同意需要是有效的同意，需要保证同意的获取是自愿、具体、清晰的，且数据主体可随时以简便的方式撤回同意；

3. 企业在涉及营销活动的数据处理时，针对数据主体的删除权、拒绝权等权利的行使一般不存在豁免条件。

※ 场景化红线

未经数据主体有效同意，禁止进行以营销为目的的个人数据处理。

03 网站公开披露个人数据四起案件

Francavilla Fontana（市政府）

※ 处罚金额

10,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 9 条

※ 处罚时间

2020/1/15

Comune di Urago（地方议会）

※ 处罚金额

4,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 9 条

※ 处罚时间

2020/2/13

Naples State Art School（学校）

※ 处罚金额

4,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 9 条

※ 处罚时间

2020/3/6

Nobel High School of Torre del Greco（学校）

※ 处罚金额

4,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 9 条

※ 处罚时间

2020/3/6

※ 案件事实概述

Naples State Art 高中在机构网站上发布的教师排名中，非法发布涉及 1,500 多名教师人员的个人信息。所涉及的教职工有关的信息具体包括家庭电话号码、手机号码、税码、居住地址和电子邮件地址等。其中还有 25 名教师涉及对其健康状况信息的收集。这些信息在机构网站上可见并可以免费下载。

Torre del Greco 高中在研究所网站上公布的教师排名中非法发布了 2,000 多名教师的健康数据和其他信息。

Comune di Urago 地方议会在其网站上发布了包含其工作人员个人数据的信息，包括健康信息。

Francavilla Fontana 市政府在其机构网站上发布了有关法院审判的信息（该市政府作为一方当事人），在相关的动机部分对申诉人的个人数据进行了披露，其中还涉及到数据主体的健康数据。这些信息在网站上可见并可以免费下载。

※ 违规分析

将涉及的个人数据公开发布在公众可获取的网站上，没有相应的合法性依据，且披露数据范围明显超出了数据处理目的，违反了数据处理的合法、公平、透明和数据最小化的原则；其中包括对健康数据的披露违反了原则上禁止披露特殊类型个人数据的规定。

※ 合规启示

1. 企业所管理的公开网站中应当避免对个人数据的披露，除非有相应的合法性基础，但也不得公开发布多余和不相关的个人数据；

2. 在这种公开渠道中，涉及健康状况等敏感个人数据的披露更是应当禁止。

※ 场景化红线

无相关合法性依据，不得在网站等公开渠道中发布个人数据。

04 某医院相关档案被非授权访问

※ 处罚金额

30,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条，第 32 条

※ 处罚时间

2020/1/23

※ 案件事实概述

该医院的实习人员和放射科医生可以访问 6 名患者的健康数据，这 6 名患者同时在该医院担任助产士。调查显示，医院采取的技术和组织措施不足以确保充分保护患者的个人数据，从而导致未经授权对患者的健康数据进行的访问。根据监管机构在 2015 年发布的健康记录指南，患者的医疗记录应当仅对涉及其健康医疗保障的医护人员开放。

※ 违规分析

该医院对患者医疗档案的管理缺乏相应的技术和组织措施，相关档案被未经授权的其他医疗人员访问，违反了数据处理安全性的规定，违反了完整性和保密性原则。

※ 合规启示

企业应当对处理个人数据的人员设置适当权限管理制度，利用适当的技术和组织措施保证个人数据的访问权限不超出授权范围，保证数据处理的安全性，尤其涉及特殊类型的个人数据。

※ 场景化红线

非经企业指示或授权的员工不得处理相关的个人数据。

05 罗马大学线上举报平台举报人个人数据被公开

※ 处罚金额

30,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条，第 32 条

※ 处罚时间

2020/1/23

※ 案件事实概述

罗马大学供其职工或第三方举报违规行为的平台，由于管理系统缺乏适当的技术访问控制措施，相关网页在没有访问控制技术措施的情况下在公共网络上公开，使得非授权人员能够访问此类数据，且未能使用加密工具来传输数据，进而泄露了两个举报人的姓名和邮箱地址。

※ 违规分析

该大学设置的线上举报平台缺乏适当的技术措施保证访问权限，使得被举报人的个人数据遭到泄露，违反了数据处理安全性的规定，违反了完整性和保密性原则。

※ 合规启示

企业在设置的违规举报途径中，应当尤其注意对举报人个人数据的保护，尤其是对线上平台的权限及安全管理方面，需要通过适当的技术和组织措施保证数据处理的安全。

※ 场景化红线

涉及处理举报人个人数据的违规举报平台不得使用安全系数较低的技术组织措施。

06 意大利电视台处理个人数据的法律依据不足

※ 处罚金额

20,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/2/6

※ 案件事实概述

该电视台播放了一部关于瑞士卖淫的纪录片，采访中的人没有得到足够的匿名。被采访人在采访中虽然面部特征被模糊化，但其在采访过程中陈述的信息均被披露，包括其原籍城市，最近装修房子和生孩子的事实，从事过的职业，不久之后将要进行的度假地点，和孩子们不久之前滑雪，指定区域以及每年去某个地方度假的习惯（明确指明）等，另外对其声音也并没有进行适当的匿名化消减，使得仍然能被部分人所识别。

※ 违规分析

该电视台在处理被采访人的个人数据时未做到充分的匿名化，相关信息涉及的个人数据向大众的传播发布没有相应的合法性基础，违反数据处理的合法、公平、透明的原则。

※ 合规启示

1. 企业在影像资料的制作过程中如果涉及个人数据的处理，需要寻求恰当的合法性基础；

2. 如果在数据主体要求进行匿名化处理时，要对影像资料进行充分的匿名处理，防止不充分的匿名化导致个人数据无适当法律依据而被处理。

※ 场景化红线

影像资料中数据主体要求匿名化处理其个人数据时，未经充分匿名化不得对外发布传播。

12 奥地利

dsb
Republik Österreich
Datenschutz behörde

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 足球教练非法收集个人数据

※ 处罚金额

1,100 欧元

※ 处罚依据

GDPR 第 6 条

※ 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。

※ 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。

※ 场景化红线

禁止偷拍行为。

02 Austrian Post数据处理的法律依据不足

※ 处罚金额

18,000,000 欧元

※ 处罚依据

GDPR 第 5（1）（a）条，第 5 条（1）（b）条，第 6 条

※ 处罚时间

2019/10/23

※ 案件事实概述

奥地利邮报创建了超过 300 万奥地利人的个人资料，其中包括有关其家庭住址，个人喜好，习惯和可能的政治偏好，这些信息随后被转售给了政党和公司等。此外还以直接营销为目的进一步处理包裹频率数据和搬迁频率数据。

※ 违规分析

将收集的数据用于与初始目的完全不同的目的，并且无新的合法性基础作为处理的依据，违反了 GDPR 第 5 条第 1 款（a）、（b）以及第 6 条的要求。

※ 合规启示

企业应严格按照初始目的进行个人数据的处理，如需使用个人数据进行不同于初始目的的处理，应满足新的合法性基础后再行处理。

※ 场景化红线

禁止在超越初始处理目的且尚未满足新的合法性基础要求的情况下进行新的处理活动。

13 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

GDPR 第 5（1）（c）条，第 9 条，第 35 条、第 36 条

※ 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。

※ 场景化红线

禁止在未进行必要性判断、目的匹配、风险评估的情况下采用人脸识别技术。

02 Nusvar AB运营的Mrkoll.se网站非法处理个人数据

※ 处罚金额

35,000 欧元

※ 处罚依据

GDPR 第 6 条

※ 处罚时间

2019/12/16

※ 案件事实概述

Mrkoll.se 网站的运营商 Nusvar AB 发布了有关所有 16 岁以上瑞典人有关违约付款的信用信息，同时发布了有关犯罪定罪记录的信息。该网站已获得相关证书，可为其大部分发布活动提供宪法保护，这意味着 GDPR 在这种情况下不适用。但对于上述两类信息，GDPR 是适用的。这种信息发布没有相关的法律依据。

※ 违规分析

该网站运营者所发布的数据主体的相关信息中关于信用信息和犯罪信息，缺乏合法性基础，违反数据处理的合法性要求。

※ 合规启示

企业所管理的公开网站中应当避免对个人数据的披露，除非有相应的合法性基础，但也不得公开发布多余和不相关的个人数据。

※ 场景化红线

无相关合法性依据，不得在网站等公开渠道中发布个人数据。

03 Google未实现数据主体被遗忘权

※ 处罚金额

7,000,000 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条，第 17 条

※ 处罚时间

2020/3/11

※ 案件事实概述

瑞典数据保护局已对 Google LLC 处以 700 万欧元的罚款，原因是该公司未能充分满足数据主体将与其有关的搜索结果从结果列表中删除的权利。

关于删除搜索结果列表的权利的事实，2014 年 5 月，欧盟法院裁定，个人可以要求搜索引擎提供商（例如 Google）删除包含个人姓名的搜索结果列表，以防该列表是不正确的，无关的或多余的。GDPR 于 2018 年 5 月 25 日生效，此权利得到了加强。但是，该权利不是绝对的，数据主体不能要求删除所有搜索结果。希望行使其要求除名的权利的个人应直接与搜索引擎提供商联系。

瑞典数据保护监管机构已在 2017 年完成了对 Google 履行将搜索结果从 Google 的搜

索引擎中删除的义务的审查，且监管机构已指示 Google 删除许多搜索结果的方式。在 2018 年，由于有迹象表明 Google 没有完全遵守先前发布的命令，监管机构发起了后续审核。这项审计现已完成，监管机构决定对 Google 处以罚款。原因是，当 Google 删除搜索结果列表时，它会以某种方式通知链接指向的网站，从而使网站所有者知道删除了哪个网页链接以及谁是删除请求背后的人。这使网站所有者可以将有问题的网页重新发布到另一个网址上，然后将其显示在 Google 搜索中。实际上，这使删除权失效，同时这种数据处理行为无相关合法性基础。

※ 违规分析

当搜索结果被删除时，Google 没有合法的依据通知网站所有者。提供信息超出了任何严格的法律义务（第 17 条第 2 款不适用）。通知网站所有者意味着个人数据的使用超出了其原始目的，这违反了 GDPR 的第 5（1）（b）和 6（4）条；而且，将相关信息通知网站所有者后，网站所有者可以将有问题的网页重新发布到另一个网址上，然后将其显示在 Google 搜索中，这实际上并未真正满足数据主体的删除权，违反了第 17 条关于删除权的规定。

※ 合规启示

企业若作为搜索引擎提供商，应当注意对包含个人姓名的搜索结果列表而言，数据主体可以行使一定的权利，比如删除权。在响应数据主体删除权请求而对搜索结果进行删除的过程中，无需将数据主体的行权信息告知相关网站的所有者。GDPR 第 17 条（2）规定的给公开个人数据的数据控制者施加通知义务，去通知那些随后通过链接、副本或复制件重新使用这些个人数据的数据控制者，不适用于搜索引擎服务提供商，因为该通知义务旨在赋予原始控制者更大的责任，并意图防止数据主体的删除请求倍增，其适用范围较窄。因此，收到数据主体删除请求的搜索引擎提供商，不需要通知在互联网上公布的信息的第三方。

※ 场景化红线

搜索引擎提供商在响应数据主体的删除权请求时，不应将删除权请求通知到搜索引擎链接指向的原始网站运营者。

04 国家政府服务中心数据泄露事件

※ 处罚金额

18,700 欧元

※ 处罚依据

GDPR 第 5（1）（f）条，第 28 条，第 32 条，33 条，34 条

※ 处罚时间

2020/4/29

※ 案件事实概述

国家政府服务中心由于 IT 系统缺乏安全保障措施发生数据泄露事件，约 282,000 名数据主体受到影响，其中 1,800 名为雇员，涉及到姓名、性别、地址、工作时间、工作地点、工作许可、社保账号、收入、纳税信息等财务信息在内的个人数据，但近 3 个月后才向数据保护监管机构报告该数据泄露事件，5 个月后才完成向数据主体告知数据泄露事件。并且，该机构没有记录关于个人数据泄露事件的有关事实、影响和采取的补救措施。此外，国家政府服务中心作为数据控制者，使用数据处理者的情况下，没有依据 GDPR 第 28 条第 3 款、第 4 款规定，与其签订有关数据处理的协议以约定数据保护义务。

※ 违规分析

该服务中心的 IT 系统缺乏安全保障，未与数据处理者签订数据处理协议进行有效的约束，造成了数据泄露，并且在发现数据泄露之后未能在

72 小时内向监管机构进行汇报，也未能立即告知数据主体，未充分履行数据泄露告知义务。没有记录与数据泄露未有关的事实。

※ 合规启示

企业应当采取适当的技术措施、对处理者进行合同约束，防止数据泄露的发生。除非数据泄露不太可能会对自然人的权利和自由造成风险，作为控制者的企业在应在发现该泄露后 72 小时内报告监管机构并立即通知数据主体，并且记录所有与数据泄露有关的事实。

※ 场景化红线

禁止不与数据处理者签订数据处理协议。禁止不及时报告数据泄露事件。禁止不对数据泄露事件进行记录。

14 比利时

GBA
Gegevensbeschermingsautoriteit

立法概况

● Data Protection Act（2018 年 7 月 30 日，规定实施 GDPR 的条款，以便进一步明确、增加或减损要求）

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 某市长非法处理个人数据

※ 处罚金额

2,000 欧元

※ 处罚依据

GDPR 第 5（1）（b）条，第 6 条

※ 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。

※ 场景化红线

禁止超越目的处理个人数据。

02 某店主过度收集客户个人数据

※ 处罚金额

10,000 欧元

※ 处罚依据

GDPR 第 5（1）（c）条

※ 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。

※ 违规分析

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。

※ 场景化红线

禁止超越目的处理个人数据。

03 某市政选举候选人超越原有目的处理个人数据

※ 处罚金额

5,000 欧元

※ 处罚依据

GDPR 第 5（1）（b）条

※ 处罚时间

2019/11/28

※ 案件事实概述

一起案件是某市政选举候选人在竞选活动中使用其职能范围内获得的联系方式进行拜票。另一起案件是某市政选举候选人利用其公共职能获得的选民名单，向其发送包括鼓励收信人投票选举候选人的信件。分别被处以 5,000 欧元罚款。

※ 违规分析

以不同于收集个人数据时的初始目的进行数据处理，违反了 GDPR 第 5 条第 1 款（b）的目的限制原则。

※ 合规启示

1. 企业应基于具体、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. 应进行权限控制，使负责相关数据处理的员工仅能按照既定的目的处理数据。

※ 场景化红线

禁止超越目的处理个人数据。

04 Website “Y” 隐私政策和cookies设置不符合要求

※ 处罚金额

15,000 欧元

※ 处罚依据

GDPR 第 4 条，第 5 条，第 6 条，第 7 条，第 12 条，第 13 条

※ 处罚时间

2019/12/17

※ 案件事实概述

法律新闻网站 “Y” 的运营商仅以英语提供隐私政策，尽管该声明也针对荷兰语和法语用户。Y 网站包含一个 “确定” 按钮来使访客同意使用 cookie，但没有设置按钮来拒绝 cookie。Y 网站运营者没有明确地给予用户拒绝同意的权利，也只是在隐私政策中提及 “通过点击 ‘更多信息’

进行拒绝”，并明确强调某些 cookie 是进行网站访问所必需的。Y 网站设置了 47 个 cookies，其中包含改进浏览功能的 cookies 也包含进行用户画像以营销为目的的 cookies，对于这些功能截然不同的 cookies，Y 网站采用的是“全有或全无”的选择模式，要么都同意使用，要不都不用。希望撤回其同意的 Y 网站的用户必须发送带有身份证明的书面或电子请求给”Y 网站“，但没有明确指出具体的联系方式。Y 网站”在其隐私声明中有如下陈述：我们的合法权益作为设置 Cookie 的法律依据，用于简化您对网站的使用并收集与使用网站相关的信息。

※ 违规分析

1. 没有考虑荷兰语和法语用户对隐私政策的需求，使得应当披露给数据主体的信息不是容易获得的，违反了 GDPR 第 5 条第 1 款（b）和第 12 条所规定的透明性原则。2.“全有或全无”的选择模式使得用户所作出的“同意”并非是自由和明确的，违反了 GDPR 第 4 条第 11 款对于同意的规定。3. 撤回同意并不像授予同意那么容易，并且因为数据主体未收到有关如何撤回其同意的足够信息，Y 网站运营者违反了 GDPR 第 7 条第（3）款关于撤销同意的规定以及第 13 条应向数据主体提供必要信息的要求。4. 在网站用户的终端设备上放置 cookie 之前进行未获得用户的同意，并且基于设置的多种不同功能的 cookie 错误地援引了“合法利益”作为设置的合法性依据，违反了 GDPR 第 5 条第 1 款（a）和第 6 条的合法性原则。

※ 合规启示

1. 隐私政策的设置应全面考虑用户所使用的语言，使隐私政策能够真正被用户容易获得；

2. 应针对不同事项分别获得用户的同意；

3. 关于撤销同意的设置应当和获取同意一样容易；

4. 隐私政策所披露的信息应完全覆盖 GDPR 第 13 条或 14 条所要求的范围；

5. 企业对于设置的 cookie 应按照 eprivacy 及 GDPR 的要求进行，针对不同类型的 cookie 选用不同的合法性基础。

※ 场景化红线

禁止不考虑用户的多样性设置单一语言版本的隐私政策。禁止不完全披露法律所要求数据主体所应了解的信息。禁止不考虑 cookie 的不同类型采用单一的合法性基础。

05 某机构没有响应数据主体的权利请求

※ 处罚金额

2,000 欧元

※ 处罚依据

GDPR 第 12 条，第 15 条，第 17 条

※ 处罚时间

2019/12/17

※ 案件事实概述

数据主体接受一种进行专门护理的非盈利组织的若干保健服务。随后数据主体收到了控制者（该非营利组织）总经理的来信，在信中通知数据主体负责为其提供服务的人员情况，此外还附上了包含了两名政治人物的该地区选举名单。在这一事实之后，数据主体试图通过寄信的方式行使其访问权，但信被退回，1 个月经过之后也没有得到任何答复。数据主体继续尝试行使被删除权，也没有得到任何回应。

※ 违规分析

控制者未在收到请求之日起 1 个月内提供其对这些请求所采取的应对措施的信息，也未告知延长的原因，没有响应数据主体的访问权和删除权请求，违反了 GDPR 第 12 条、15 条和 17 条。

※ 合规启示

1. 企业应保证其向数据主体披露的联系方式是有效的；

2. 企业应在规定的时间范围内对数据主体的权利请求作出响应，如因考虑到请求的数量和复杂性，因及时告知数据主体延迟的情况。

※ 场景化红线

禁止不及时响应数据主体的权利请求。

06 Proximus SA的数据保护官任命不符合法律要求

※ 处罚金额

50,000 欧元

※ 处罚依据

GDPR 第 31 条，第 37 条，第 38 条

※ 处罚时间

2020/4/28

※ 案件事实概述

在一起数据泄露事件处理中，监管机构发现电信运营商 Proximus SA 的数据保护官（DPO）参与不足，经进一步调查评估，监管机构认定 Proximus SA 的 DPO 对于数据保护治理工作只是知情，而非充分、及时地参与并提供咨询意见。该 DPO 同时担任有利益冲突的多种职务，同时承担合规、风险管理和内部审计职责，且该公司缺乏组织性、系统性措施防止 DPO 职务间的利益冲突。此外，该公司还未能在监管机构调查过程中充分履行与监管机构合作的义务。

※ 违规分析

DPO 未充分、恰当、及时参与数据保护工作；DPO 多种职务间存在利益冲突，无法保证数据保护官的独立性；没有遵守与监管机构合作的义务。

※ 合规启示

企业在为 DPO 设置职务或工作时应注意各项工作内容是否有利益冲突，应当确保 DPO 可以独立地履行各项职责。企业应积极配合监管机构进行各项调查。

※ 场景化红线

禁止为 DPO 设置多项有利益冲突的工作。

15 挪威

Datatilsynet

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 某市政府数字学习平台数据处理安全性不足

※ 处罚金额

73,600 欧元

※ 处罚依据

GDPR 第 5（1）（f）条，第 32 条

※ 处罚时间

2020/2/26

※ 案件事实概述

该市政府在 Showbie 数字学习平台中处理了 15 名肢体和精神残疾儿童的健康信息，以便在学校与其家庭之间传递与健康有关的个人信息。监管机构发现，在使用该应用程序之前，没有进行必要的隐私影响评估或测试，并且登录该应用程

序时缺乏适当的安全保障措施，使得可以访问小组中其他学生的信息。

※ 违规分析

该市政府运营的数字学习平台处理儿童的健康信息，在投入使用前未进行必要的数据保护影响评估，同时未能提供适当的技术措施保证数据的访问权限，导致非授权访问其他学生的信息，违反了数据处理安全性的规定，违反了完整性和保密性原则。

※ 合规启示

企业应当对处理个人数据的人员设置适当权限管理制度，利用适当的技术和组织措施保证个人数据的访问权限不超出授权范围，保证数据处理的安全性，尤其涉及特殊类型的个人数据。

※ 场景化红线

禁止对个人数据设置超出授权范围的访问权限。

02 某公司非法处理儿童个人数据

※ 处罚金额

36,800 欧元

※ 处罚依据

GDPR 第 5 条，第 6 条

※ 处罚时间

2020/2/28

※ 案件事实概述

Coop Finnmark SA 下的一家商店因传播了摄像头捕捉的涉及儿童的图像信息而被挪威数据保护监管机构处罚。录像显示，四个孩子的年龄估计为 15 或 16 岁，其中两个孩子进行了盗窃，另外两个孩子在旁边看着。商店经理用自己的手机在屏幕上拍摄了录像，然后将其发送给他的熟人，并询问“这是您的儿子吗？”。这位女士的回答是否定的，但随后将录像传递给了她的儿子，录像最终传递到多人手中。

※ 违规分析

摄像头捕捉的儿童图像信息，经过传播，披露给了不确定的很多人。这种数据处理没有合法性基础，违反了数据处理的合法性原则。

※ 合规启示

企业在处理的视频监控设备中的图像信息时，应当采取必要的技术组织措施防止相关信息被非法传播，尤其关注防止通过个人移动通信设备进行再处理，从而导致数据信息不受控的传播。

※ 场景化红线

禁止将视频监控设备中的图像类个人数据通过任何手段披露给非授权第三方人员。

16 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

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

GDPR 第 5（1）（e）条，第 5（2）条

※ 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。

※ 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。

※ 场景化红线

禁止超越必要的时间存储个人数据。

02 Hørsholm市工作电脑被盗导致数据泄露

※ 处罚金额

7,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条，第 32 条

※ 处罚时间

2020/3/10

※ 案件事实概述

一名市政府雇员的工作计算机被盗，其中包含大约 1600 名市政府雇员的个人数据，包括敏感信息和有关社会保险号的信息。

※ 违规分析

市政当局处理其雇员相关的个人数据，未能采取适当的技术组织措施，使得计算机被盗后，其中存储的大量的雇员个人数据有泄露的风险，这违反了数据处理的安全性规定，违反了完整性和保密性原则。

※ 合规启示

企业使用的计算机应当做好加密和备份措施，防范计算机丢失或损坏后，其中的个人数据产生数据安全性风险。

※ 场景化红线

禁止将个人数据不加备份或无任何保密措施地存储在员工使用的笔记本电脑中。

03 Gladsaxe市工作电脑被盗导致数据泄露

※ 处罚金额

14,000 欧元

※ 处罚依据

GDPR 第 5（1）（f）条，第 32 条

※ 处罚时间

2020/3/10

※ 案件事实概述

一台包含不受加密保护的个人数据的计算机被盗，其中包括 20620 名城市居民的敏感信息和个人识别号码。

※ 违规分析

市政当局处理有关市政公民的大量个人数据，包括敏感信息。公民不能拒绝市政当局处理有关其信息，因此，市政当局对其处理的个人数据的安全性承担重大责任。当个人数据存储在计算机本地时，更应通过加密措施保证数据的安全，市政府的行为违反了数据处理的安全性的规定，违反了完整性和保密性原则。

※ 合规启示

企业使用的计算机应当做好加密和备份措施，防范计算机丢失或损坏后，其中的个人数据产生数据安全性风险。

※ 场景化红线

禁止将个人数据不加备份或无任何保密措施地存储在员工使用的笔记本电脑中。

17 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 三家公司数据处理的合法性依据不足

※ 处罚金额

70,000 欧元； 10,000 欧元；2,000 欧元

※ 处罚依据

GDPR 第 6（1）（f）条，第 9 条

※ 处罚时间

2019/10/25

※ 案件事实概述

LGS Handling Ltd, Louis Travel Ltd, 和 Louis Aviation Ltd 这三家公司使用“布拉德福德因子”（Bradford Factor）对与员工有关的病假

的日期和频率等数据进行评分并根据结果对个人进行分析，公司选取合法利益作为数据处理的合法性基础，并进行了影响评估，但在评估中未证明其利益高于员工的利益。

※ 违规分析

监管机构认为在员工的身份已经被直接或间接披露的情况下，处理与其有关的病假日期和频率，属于对个人数据的处理，而且是对健康这类特殊类型个人数据的处理。即使进行了影响评估，但在该评估中没有能够证明公司的利益高于员工的权利和自由，所以合法利益不成立。此外不属于 GDPR 第 9 条规定的对特殊类型个人数据处理的任何一种例外。

※ 合规启示

企业在以合法利益为合法性基础处理个人数据时应证明其合法利益高于数据主体的权利和自由。

※ 场景化红线

禁止在进行利益平衡测试之前使用合法利益作为合法性基础。

02 某公司未获同意发送营销信息

※ 处罚金额

1,000 欧元

※ 处罚依据

GDPR 第 5（1）（a）条，第 6 条，第 21 条

※ 处罚时间

2020/1/13

※ 案件事实概述

该企业在未获得数据主体同意的情况下向其发送 eShop for Sports 的 SMS 营销信息，并且该信息中未提供一个免费的电话来拒绝接受此消息。有数据主体向 SMS 的编辑方发送了投诉但未得到回应并且仍然继续收到该营销信息。该企业回应称投诉人的号码已被删除，但是因为技术问题 SMS 提供者的系统没有很好地运转，所以仍然继续收到改营销信息。此外该系统未提供一些免费的自动终止接收消息的操作。

※ 违规分析

该企业在未获得数据主体同意的情况下发送营销信息，且未能约束其处理者保障数据主体拒绝权有效的行使。

※ 合规启示

1. 企业应在充分分析营销信息内容的基础上选择和满足相应的合法性基础要求；

2. 企业应对其供应商进行有效约束保障数据主体的权利实现。

※ 场景化红线

禁止在不具备合法性基础的情况下向数据主体发送营销信息。

18 冰岛

PERSÓNU VERND

立法概况

● 第 90/2018 号法案《数据保护及个人数据处理》

监管机构

The Data Protection Authority (Icelandic: ‘Persónuvernd’)

网址：www.personuvernd.is

E-mail: postur@personuvernd.is

电话： +354 510-9600

01 某教师错误发送学生访谈资料

※ 处罚金额

9,000 欧元

※ 处罚依据

GDPR 第 5（1）f）条，第 32 条

※ 处罚时间

2020/3/10

※ 案件事实概述

2019 年 8 月 15 日，Breiðholt Upper Secondary School 的一名教师错误的将上一年的访谈资料当做访谈时间安排发给了新生及其监护人，访谈资料中包含敏感数据。

※ 违规分析

该教师的错误操作使得敏感数据遭受了非授权访问，属于数据泄露，违反了数据完整性和保密性原则、数据安全的要求。

※ 合规启示

企业应采取适当的组织措施保障数据安全，提升授权处理个人数据的员工的数据保护意识，防止因错误发送导致的数据泄露。

※ 场景化红线

禁止错误地发送含有个人数据的文档。

02 SAA错误发送病人资料

※ 处罚金额

20,600 欧元

※ 处罚依据

GDPR 第 5（1）f）条，第 32 条

※ 处罚时间

2020/3/10

※ 案件事实概述

2018 年秋天 National Center of Addiction Medicine ('SAA') 的一名已经在前一年离职的员工收到了含有大量病人信息的一箱资料，其中包括约 3000 名病人姓名的入住登记簿和 252 个人的详细病历。

※ 违规分析

将个人数据寄送给前员工属于使数据遭受了非授权访问的情形，属于数据泄露。 S.Á.Á 缺乏安全保障措施防止数据泄露，违反了数据完整性和保密性原则、数据安全的要求。

※ 合规启示

企业应采取适当的组织措施保障数据安全，提升授权处理个人数据的员工的数据保护意识，防止因错误发送导致的数据泄露。

※ 场景化红线

禁止错误地发送含有个人数据的文档。

19 克罗地亚

azop
Agencija za zaštitu osobnih podataka

立法概况

● 《实施一般数据保护条例法》（克罗地亚语为 Zakon oprovebiOpćoeredbeozaštitipodataka，该法案于 2018 年 5 月 25 日正式生效）

监管机构

Croatian Personal Data Protection Agency（DPA）

网址 : https://azop.hr/

英 文 主 页：https://azop.hr/data-protection-agency

E-mail: azop@azop.hr

电话：00385 (0)1 4609-000

传真： 00385 (0)1 4609-099"

01 某银行没有保障数据主体的访问权

※ 处罚金额

10,000 欧元

※ 处罚依据

GDPR 第 15（3）条

※ 处罚时间

2020/3/13

※ 案件事实概述

在 2018 年 5 月至 2019 年 4 月期间，该银行拒绝向其客户提供信贷文件副本（例如，还款计划，贷款协议附件，利率变动审查等）。在根据数据主体的投诉启动的程序中，监管机构命令银行响应访问权并提供所请求的贷款文件的副本。在处以罚款时，监管机构特别考虑到该银行未能遵守所下令的措施，该银行实行这种做法将近一年，并拒绝获得其 2500 多个客户的访问权。

※ 违规分析

该银行拒绝向数据主体提供信贷文件副本，没有保障数据主体的访问权。

※ 合规启示

企业应及时响应数据主体的权利请求。

※ 场景化红线

禁止延迟或无合法理由拒绝响应数据主体的权利请求。

案例索引

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。

《GDPR 执法案例全景白皮书（2019-2020）》是立足《GDPR 执法案例精选白皮书（2018-2019）》已有基础的更新与发展，全景收录了 GDPR 生效第二年中绝大多数公开案例，由中兴通讯数据保护合规部发布。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。

编者：王业美、石墨翰、徐敏、吴以源、高瑞鑫、甘亚棋