欧盟 GDPR 合规指引

二〇一九年五月

编写团队

编写单位：

中国信息通信研究院安全研究所

对外经济贸易大学数字经济与法律创新研究中心

奋迅律师事务所

科文顿·柏灵律师事务所

京东集团

北京大学法治与发展研究院

编写组成员：（姓氏笔画为序）

于智精、许可、严少敏、罗嫣、陈湉、吴薇、洪延青、胡翔、葛鑫、鲍治、魏亮

版权声明

序　　言

如何把握欧盟的《通用数据保护条例》（GDPR）？如果不拘泥于具体条文的话，我总觉得答案其实就蕴含于这座烧毁断残的雕像之中。

这座雕像位于荷兰乌特勒支大学学术大厅的走廊。保留至今为的是纪念二战期间五名荷兰学生的英雄之举。1942 年 12 月 12 日深夜，Gijs den Besten、Frits Lordens、Geert Lubberhuizen、Anne Maclaine Pont 和 Rutger Marthijsen 潜入这座雕像背后的学生管理部，将大学当时保存的学生档案一把火全部烧毁，避免了当时占领荷兰的德国纳粹通过详尽的学生档案锁定并杀害犹太学生。

“即便在最黑暗的时刻，我们仍然知道存在着永恒的原则”（In de zwartste uren bleven wij weten, dat er eeuwige beginselen zijn）。乌特勒支大学教授 dr. P. C. A. Geyl 这句总结，连同焦黑断裂的雕像，给每个驻足探究的人，

包括当时即将博士论文答辩的我，深深的震撼和思考。如果德国纳粹掌握了这些学生档案（其实就是学生的个人数据），会有多少人将因此而丧生；但当时欧洲范围内又有多少人像乌特勒支大学中的犹太学生那般幸运，能够有机会销毁自己的个人数据……

二战血和泪的经历显然在欧洲人的心中刻下了一个教训：人人都应当享有个人数据受保护这项基本人权；个人数据泄露或滥用所造成的危害，绝非财产上的损失，而是事关个人的尊严和人格，乃至生命。

就此，我们不难理解 GDPR 这样严格的个人数据处理活动法律框架，为什么会诞生于欧洲。从本质上来说，GDPR 代表了欧盟所作出的价值判断：个人数据无论是为政府还是企业所掌握，难免出错；GDPR 不仅是为了最大程度降低“重蹈覆辙”的风险，更是面对未来科技迅猛发展的基本立场——人是科技的主人，科技应当在尊重人类福祉的框架中发展进步。

沿着这样的脉络，我们就能掌握 GDPR 所设立的基本原则和具体的制度设计，例如开展个人数据处理活动首先需要一个合法性基础；对处理活动非常高的透明性和文档化要求：事先明确数据处理的目的；仅能收集目的所需的最小化的个人数据；个人数据的存储不应超过实现目的所必需的时间；开展高风险的个人数据处理活动前应当开展影响评估；产品或服务在开发设计阶段就应落实数据保护的要求；对违法处理活动施加高额的罚款等等。

除了“不信任”对开展个人数据处理活动的组织，GDPR 还赋予了个人在个人数据方面的前所未有权利。在经典的查询、更正、删除权利的基础上，个人还拥有更强的反对、免受系统完全自动化决定的权利，以及崭新的被遗忘权、限制处理权和数据可携带权。在这些权利的“武装”之下，个人不再是被动地“受制于”控制其数据的组织，而能及时、简便、深入地参与、介入，甚至于干预组织所开展的数据处理活动。除非有法定事由等少许例外情形，组织无法将个人拒之门外。

一边给开展个人数据处理活动的组织带上了沉重的“镣铐”，一边大幅度给个人赋权，GDPR 通过上述“双保险”，以管控个人数据处理活动对个人合法权益可能带来的负面风险。这样的设计是欧盟国家集体作出的抉择，是欧盟价值观的逻辑展开。

反观中国，个人信息保护法的立法工作已经吹响了号角。我们与欧洲有着不同的历史和传统，处于不同的发展阶段，形成了不同的政治、社会和经济结构。

显然，中国无需追随欧盟的步伐，但这并不意味着将 GDPR“掰开揉碎”搞清楚没有意义。至少，GDPR 针对普适性问题提出的解决方案，我们可以批判、借鉴，并在此基础上创新。

本着这样的根本目的，同时为满足在欧盟运营的我国企业的实际需求，一群来自于高校、政府智库、企业、律所等方面的专家在中国信息通信研究院安全研究所提供的平台上齐聚一堂，根据自己的研究和实践经验，并经过长达半年的准备、讨论、撰写、修改、审校，集体创作出这份《GDPR 合规指引》。

这份指引共分四章，分别包括 GDPR 概述、合规体系、疑难点及合规建议，以及 GDPR 与我国法律的比较及冲突应对。我们希望能为有合规需求的企业指明方向，更希望能为关心个人信息保护的同仁提供一份针对 GDPR 准确、客观、扎实的介绍，进而为我国开展个人信息保护工作贡献绵薄之力。

目　录

一、GDPR 概述

（一）GDPR 立法背景及进程

欧盟的个人信息保护起源于传统隐私保护，发展至今先后历经以《1981 年个人数据保护公约》、《1995 年个人数据保护指令》（以下简称“95 指令”）以及 2016 年《通用数据保护条例》（英文简称“GDPR”）为主要表现形式的三个阶段。在互联网和大数据崛起的新环境下，欧盟认为 95 指令不能切实保护数据主体的权利和自由，也不能对成员国之间的个人数据保护法加以协调。因此，自 2009 年开始，欧盟启动个人数据保护框架的改革工作。此次数据保护改革的宗旨在于强化数据主体权利的保护，并统一欧盟各成员国的数据保护立法。经过公众意见咨询、利益相关者对话和备选政策的影响效果评估，欧盟委员会最终决定以条例形式取代 95 指令，并于 2012 年 1 月正式发布 GDPR 草案。经过长达四年的立法程序，2016 年 4 月，欧盟理事会和欧洲议会表决通过了 GDPR，并随后在 2016 年 5 月 4 日正式在欧盟官方公报发布。根据 GDPR 第 99 条关于生效和适用的规定，GDPR 自官方公报发布满 20 日，即 2016 年 5 月 24 日生效，并自其生效后满两年，即 2018 年 5 月 25 日直接适用于欧盟全体成员国，以“一个大陆、一部法律”实现在欧盟 28 个成员国内部建立起统一的个人信息保护和流动规则。由于 GDPR 的域外适用效力，被称为史上最严数据保护法的 GDPR 在全球范围内引起广泛关注。

（二）GDPR 制度要点概述

相较于 95 指令 GDPR 在地域适用范围、权利义务配置、监管体系设计等方面进行了较大调整。

1、扩张域外适用效力

相较于 95 指令依据传统管辖权原则确认适用范围，为应对网络空间无国界的特征和数据跨境流动常态化的现状，GDPR 超越了一般以属地管辖为主、属人管辖为辅的原则，而从更为抽象的意义上将所有涉及欧盟地区数据主体个人数据处理的行为均纳入了管辖范围。GDPR 在第 3 条中规定了“属人”、“属地”、“保护”、“国际公法”等多种管辖权适用依据：其一，第 3 条（1）规定 GDPR 适用于数据控制者或处理者在欧盟境内的实体机构实施的个人数据处理行•为，不论数据处理行为是否发生在欧盟境内。根据 GDPR 序言第 22 条，对于是否存在欧

盟境内实体机构或营业场所的判断，只要是通过稳定的安排能够真正有效的开展活动即可，不拘泥于分支机构抑或是子公司的法律形式。同时，欧盟法院 Google 被遗忘权一案中认为明确此时数据处理活动不限于实体机构自身实施，而只要是在实体机构“活动背景下”（in the context of the activities）实施即可。欧洲数据保护委员会（European Data Protection Board）认为只要实体机构与数据控制者或处理者之间存在着“无可摆脱的联系”，则数据控制者或处理者实施的数据处理行为（无论是否发生在欧盟境内）均应受 GDPR 的拘束。其二，第 3 条（2）依据保护原则规定即便数据处理者、控制者以及数据处理行为均不发生在欧盟境内，但为了保护欧盟及欧盟境内居住的数据主体的合法权益，只要向欧盟数据主体提供产品或服务或监控其行为的个人数据处理行为，均应受到 GDPR 的拘束。其三，第 2 条（3）条规定虽然数据控制者设立在欧盟境外，但依据国际公法，其所在地区适用欧盟成员国法律时，其行为也受到 GDPR 拘束。

2、扩张数据主体权利

GDPR 第三章专章（第 12 条-第 23 条）规定了数据主体的权利，包括透明度及模式、知情与对数据的访问、更正与删除、反对权和自动化决策、权利限制等五个部分的内容。相较于 95 指令所规定的数据主体权利，GDPR 在以数据主体“知情——同意”为基本框架，保留、细化并拓展了 95 指令中已有的查询、更正、删除、反对、免受完全自动化决定权等数据主体权利体系，并新增了被遗忘权、限制处理权和数据可携带权。

具体来看，第 12-15 条构成数据主体的知情权体系，第 12 条规定透明性原则明确数据主体有权要求数据控制者以易于获取和易于理解的形式及时提供数据处理的相关信息，构成数据主体其他逐项权利行使的前提条件；第 13 条、第 14 条分别列举了在个人数据直接收集和间接收集的不同场景下，数据控制者应当为信息主体提供的各项信息的具体内容，构成对第 12 条透明性原则的细化和体现。第 15 条规定了数据主体的访问权，明确数据主体有权从数据控制者处明确是否对其个人数据进行了处理，并要求数据控制者提供正在处理的个人数据副本。

第 16 条-第 20 条规定了数据主体的更正权和删除权体系。其中，第 16 条更正权是 95 指令中既已存在的权利，赋予数据主体纠正其错误个人信息的权利。第 17-第 20 条所规定的被遗忘权、限制处理权和数据可携带权，则是 GDPR 应因网络社会数据记录和处理自动化的常态而新增的数据主体权利。被遗忘权（第

17 条）来源于 95 指令中的删除权，但又融入了数字时代的背景，其行使范围不限于传统删除权中数据存在错误或者欠缺法定或约定处理依据的情形，而是可以涵盖在合法基础上进行的数据处理，其判断标准在于数据相对于其处理目的是否为过时的、不相关的、不必要的信息，但其行使的范围受限于具体场景下与言论自由、公共利益等的利益平衡。限制处理权（第 18 条）则赋予数据主体在数据的准确性存疑需要进一步查证、数据处理并无合法依据但数据主体并不希望删除其数据等情形时，有权限制数据控制者对其个人数据的处理，一旦数据行使该项权利，则仅在数据主体同意或者为保护其他自然人或法人的权利等特殊情形才得进一步处理个人数据。相较于被遗忘权，限制处理权提供了相对缓和的解决方案。可携带权（第 20 条）也旨在强化数据主体对其个人数据的控制权，其基本理念在于“个人能够将其个人数据和资料从一个数据控制者处无障碍地转移至另一个数据控制者处”，由于该权利大大降低了数据主体转移其个人数据的难度，也被认为能够进一步提升数据控制者之间的市场竞争程度，从而促进数据控制者的创新发展。

第 21-22 条规定了数据主体的反对权和自动化决策相关内容。反对权（第 21 条）是对 95 指令针对数据商业利用的反对权的保留和延伸，相较于原有 95 指令中的规定，GDPR 对于反对权的规定放宽了适用情形，不再局限于商业利用场景，包括基于维护公共利益或数据控制者所追求合法利益所必需、基于直接营销目的、基于科学研究或统计目的的数据处理的场景，均有反对权的适用可能。免受自动化决策权（第 22 条）明确对数据主体具有法律影响或类似重大影响的基于数据自动化处理的相关决策，数据主体有权拒绝其约束。免受自动化决策权的基本出发点在于大数据时代数据自动化处理和对数据主体进行定向分析的数据画像日益增多，但算法不透明、算法歧视、数据源错误等风险难以避免，因此有必要在其对数据主体产生重大影响时，赋予数据主体免受其限制的权利。

第 23 条则规定了数据主体权利的限制。从数据主体权利与公共利益、他人合法利益等多元利益冲突格局出发，第 23 条赋予成员国在基于维护国家安全与防卫、公共安全等公共利益情形下，在符合基本权利的自由和本质并提供了必要适当保护措施的前提下，对数据主体的权利进行限制，以协调数据主体权利与诸项公共利益。

3、强化数据控制者、数据处理者问责

GDPR 在引入一站式监管机制降低数据控制者等企业日常合规负担的同时，也要求数据控制者、数据处理者内部建立完善的问责机制，更多地以企业内部合规性义务规定推进 GDPR 的落地。具体来说，该等规范主要体现在设置数据保护官、对数据处理活动实现文档化管理、实行数据保护影响风险评估制度、对高风险数据处理活动向监管机构事先咨询、向监管机构和数据主体进行数据泄露事件的报告和通知、强调匿名化与假名化安全保障措施等等。除此之外，GDPR 与 95 指令显著不同之处还在于 GDPR 考虑到大数据、云计算产业的诸多业务发展需求，在大多数情况下明确了数据处理者与数据控制者负有同等义务，并且明确数据处理者在数据安全、数据泄露、数据保护影响风险评估等方面对数据控制者负有协助义务，以及数据处理服务终止时的数据删除或返还义务。

4、丰富数据跨境流动机制

为应对日益增长的全球跨境流动和 95 指令体系下监管体制之间的不协调，欧盟在此次数据保护改革中着力数据跨境传输机制进行了完善，重点在于提升数据跨境流动监管政策的流动性，明确禁止成员国数据跨境流动监管许可的适用，并且注重发挥行业协会等社会监督和市场自律作用，最终形成了基于充分性决定、有拘束力公司规则、标准合同条款、经批准的行为准则、经批准的认证机制或标志等构成的多元数据跨境流动监管路径，实现用户隐私、数据安全与数据跨境流动需求之间的协调与平衡。

5、改革数据保护监管体制

为确保 GDPR 在适用过程中能实现对不同成员国之间的协调，相较于 95 指令的监管体系，GDPR 在监管机构、监管模式、监管手段等方面均作出了重大变革。在整个欧盟层面，GDPR 的首要变化在于设立欧盟数据保护委员会（European Data Protection Board，EDPB）取代 95 指令下的第 29 条工作组（WP29），EDPB 由各成员国数据保护监管机构负责人和欧盟数据保护专员（EDPS）组成，负责代表整个欧盟层面发布有关个人数据保护的相关意见、指南，协调一站式监管机制并促进交流等，以确保 GDPR 在欧盟各成员国内适用的统一性。除此之外，GDPR 新增监管一致性机制，以应对跨境数据流动场景下涉及多个成员国监管机构的情形，减轻监管成本和企业合规成本，力图实现一站式管理服务。在一致性机制下，当涉及多个监管机构时，则需要区分主导监管机构和相关监管机构，由

主要营业地的数据保护监管机关作为主导监管机关，数据控制者等监管对象只需向主导监管机构履行相关义务，由主导监管机构及时将相应监管事项通知其余相关监管机构，后者仅在有限的紧急情况下才得对其领土内的被监管对象采取措施，从而避免被监管对象对接多个成员国监管机构。

（三）GDPR 执法行动及评估

1、GDPR 执法行动

（1）EDPB 与各国监管机构的职能与权限

欧盟数据保护委员会（“EDPB”）是整个欧盟层面的数据保护机构，旨在保证欧盟整体数据保护规则的统一适用，以及促进各成员国数据保护监管机构之间的合作，其主要政策工具为出台指南（Guidelines）、建议（Recommendations）、意见（Opinions）以及有约束力的决定（Binding decisions）。GDPR 正式生效后，EDPB 在 2018 年 5 月 25 日举行了第一次全体会议。会上集中完成 EDPB 的设立工作，经选举产生了委员会主席和副主席；同时会上还完成了 WP29 与 EDPB 的交接，批准了 16 个 WP29 与 GDPR 有关的指南。

与 EDPB 相对，各国监管机构的职能与权限由本国数据保护法赋予，其权限主要包括调查权和矫正权。具体而言，监管机构可通过发出违规警告、开展审查、限期纠正、命令删除数据、暂停向第三国传输数据、罚款等行使其权力。

（2）EDPB 相关行动

2018 年 7 月 4 日—5 日，EDPB 举行了第二次全体会议，会议涉及一站式（One-Stop-Shop）合作机制、ICANN、PSD2 指令、隐私盾等广泛主题。根据欧洲数据保护专员公署（EDPS，EDPB 的常设秘书处）目前的工作设想，后续执法要点主要包括：

i. GDPR 实施工作的基本立场是遵循欧盟委员会有关数字单一市场的总体安排，以保护欧盟公民和统一市场为直接目标指向；
ii. 贯彻落实 GDPR 规范内容的主要切入点是里斯本条约等确认的个人数据权等“基本权利”的保护，由此后续设计更为具体的实施细则以及合规指南；

iii. 关于 GDPR 的具体执法力度，依据欧盟委员会目前确定的口径，总体强度将类似于欧盟目前有关反不正当竞争、反垄断领域的执法力度；

iv. 在执法机制上，GDPR 的执法凭借主要是各国监管机构，但强调“一站式”执法模式，也即由某执法对象（例如跨国公司）主要营业地的成员国监管机构履行主要的监管职能；

v. 在国际冲突博弈方面，由于 GDPR 的域外管辖条款是全新的制度设计，预计在实施过程中会遇到较大的反弹，目前主要外部压力来自美国和英国方面，为此 GDPR 实施过程中会根据实际情况进一步考虑弹性的执法机制，例如充分发挥“公司规则”(Rules of Corporation)和“标准条款”（Standard Clause）两项机制的弹性功能，以减少法定强制条款（例如“充分性认定”机制）的适用情形。

2019 年 2 月，EDPB 发布 GDPR 实施情况首次概述，对各国相关监管机构的合作机制（Cooperation mechanism）与一致性机制（Consistency mechanism）的实施与执行情况进行总结。

合作机制指利用一站式合作机制、互助、联合执法等工具支持跨境案件的执行。合作往往在各国监管机构层面开展，除非机构之间出现纠纷或者有紧急情况，EDPB 不会介入。为便于 GDPR 在欧洲层面的执法，EDPB 利用内部市场信息 IT 系统（“IMI 系统”）为各监管机构之间提供结构化且保密性的信息共享。根据 IMI 系统，自 2018 年 5 月 25 日至 2019 年 2 月 26 日，跨境案件的总数为 281 起，主要涵盖数据主体权利行使、消费者权、数据泄露等主题。已经发起 642 个确定牵头监管机构与相关监管机构的初始程序，其中 306 起已完成并确定出牵头监管机构，尚未出现关于牵头监管机构确认的纠纷。14 家欧洲经济区国家的监管机构发起 45 个一站式程序，其中 23 个处于信息协商阶段，16 个处于起草决定阶段，6 个已发布最终决定。可以预见，一站式程序的数量在未来将稳定增长。在互助程序方面，18 家监管机构共发起 444 件互助请求（包括正式和非正式请求），其中 353 件请求在 23 日内得到回复。在联合执法方面，目前尚未有联合执法程序被发起。

一致性机制涵盖 EDPB 为确保 GDPR 在各监管机构间适用与执行的一致性而出台的一般指南，以及意见、决定、争议解决与紧急决定等。迄今，EDPB 已发布六部指南（含征求意见稿），涵盖地域范围、认证机构、行为准则等主题；发布 28 个成员国应接受数据保护影响评估的处理主体名单的一致性意见，以及其他与金融监管机构个人数据传输行政安排、GDPR 与《隐私与电子通讯指令》

的关系等主题相关的一致性意见。约束性公司规则、数据控制者与数据处理者协议相关的意见将后续发布。

（3）各国监管机构执法行动

在 GDPR 生效后过渡期和正式施行以来，欧盟内不少成员国也从国内立法和监管执法等方面作出回应。从立法层面上来看，为应对 GDPR 对 95 指令的改革和变化爱尔兰、奥地利、希腊等国家对现有个人数据保护法规作出修订，出台了相应的修订法案。从监管执法层面上来看，多数成员国监管机构收到的投诉以及发起的调查大幅增加，31 家监管机构报告的案件总数达 206,326 起，可分为基于投诉的案件、基于数据泄露报告的案件及其他类型案件，其中 51%的案件已结案，1%的案件被上诉至国内法院。此外共 11 家监管机构根据 GDPR 第 58.2(i)条进行罚款，罚款总额达 55,955,871 欧元。

i. 爱尔兰

根据爱尔兰数据保护监管机构 DPC 于 2019 年 2 月底发布的年度报告，DPC 在 2018 年共收到 1,928 起 GDPR 相关投诉，其中 868 起已结案。大部分投诉通过友好协商方式解决，18 起投诉以 DPC 发布正式决定的方式结案。在数据泄露方面，共有 3,542 起数据泄露事件被记录在案，其中 38 起事件涉及 11 家跨国科技公司。此外，DPC 继续担任 11 家公司约束性公司规则申请的主要审阅机构。

由于爱尔兰是包括多家大型科技与社交媒体公司在内的许多跨国公司的欧洲总部（也即“主营业地”）所在地，DPC 在对欧洲地区跨国公司的数据保护监管中特别是在一站式机制下发挥着重要作用。DPC 通过一站式机制接收的跨境投诉案件共有 136 起，其中关于“同意”、“删除权”和“访问权”的投诉占比较大。作为苹果、脸书、微软、推特、爱彼迎、领英等案件在一站式机制下的牵头监管机构，DPC 已发起 15 起涉及这些跨国科技公司的法定调查，且收到了 16 起来自其他欧盟监管机构的与跨国科技公司相关的互助请求。DPC 开展调查所涉主要问题包括脸书涉嫌利用外部链接从第三方软件中转移个人数据至脸书即其合作方、微软利用 Office 产品收集并处理遥测数据、WhatsApp 与其他脸书公司共享个人数据等等。

ii. 英国

根据英国数据保护监管机构 ICO 官网数据，ICO 自 GDPR 生效以来共有 59 项执法行动，其中 34 项为罚款，15 项为执行通知。

2018 年 10 月，ICO 向一家加拿大数据分析公司 Aggregate IQ 数据服务有限公司（“AIQ”）发出执行通知，要求其删除所有与英国公民相关的个人数据，并称若其不履行义务，将面临最高 2000 万欧元或上一年全球总营业额 4%的罚款。AIQ 是一家利用个人数据在社交软件定向投放政治广告的公司，由包括脱欧组织在内的政治团体提供个人数据。ICO 在执行通知中指出 AIQ 违反了 GDPR 第 5(1)条中的(a)至(c)款，与此同时，加拿大隐私监管机构也在以滥用个人数据对 AIQ 进行调查。在 ICO 缩小了执行通知中的范围后，AIQ 撤销了上诉请求。

在后续的执法行动中，ICO 还对脱欧集团有限公司（Leave.EU Group Limited）、投票脱欧有限公司（Vote Leave Limited）的非法利用数据和发送信息行为处以罚款。

iii. 法国

根据法国数据保护监管机构 CNIL 于 2019 年 4 月发布的 2018 年活动报告，2018 年 CNIL 共收到 11,077 起投诉（相较于 2017 年上涨了 32.5%），其中 20%为一站式机制下来自其他监管机构的投诉。这些投诉主要涉及数据的互联网传播，尤其是要求个人数据的删除，涵盖线上声誉、市场/商业、人力资源等领域。在调查方面，CNIL 在 2018 年共发起 310 其调查；在发布命令与实施处罚方面，CNIL 在 2019 年发布的 49 项命令主要集中在保险领域和利用科技的广告定向投放领域，共实施了 11 项处罚，其中 10 项为罚款。

2019 年 1 月 21 日，CNIL 对谷歌作出了 GDPR 下至今最高额的罚款处罚——5 千万欧元。CNIL 的处罚决定理由主要基于两方面，一是谷歌违反了 GDPR 第 12 和 13 条规定的透明度要求，二是谷歌以广告定向投放为目的处理个人数据缺乏法律基础，即未获得数据主体的有效同意。此外，该决定认为谷歌在欧盟境

内的主营业地不在爱尔兰，而是没有主营业地，因此 CNIL 是实施处罚的适格主体。

iv. 其他各国

a) 德国监管机构 BfDI 基于数据泄露对一家社交媒体公司处以 2 万欧元罚款；
b) 意大利监管机构 Garante 就两家公司车辆的定位监控系统问题发出执行通知要求其纠正违法行为；
c) 葡萄牙数据监管机构（CNPD）认定 Barreiro 医院未区分临床数据的访问权限，并且在个人资料管理系统上存在缺陷，违反了 GDPR 第 51)f)条的“完整性和保密性”原则与 51)c)条的“数据最小化”原则，对其处罚 40 万欧元；
d) 立陶宛监管机构 SDPI 对一家互联网支付公司处以 61,500 欧元罚款，理由包括不恰当处理数据、泄露个人信息以及未向监管机构报告数据泄露事件；
e) 奥地利数据监管机构（DSB）因企业在其建筑物周边安装闭路监控设备监控、记录人行道人像数据等，而被认为未履行 GDPR 有关数据处理透明度的要求，对其处罚 4800 欧元；

2、GDPR 执法行动评估

在 EDPB 与欧洲各监管机构执法合作方面，GDPR 下建立的合作与一致性机制进展相对顺利。鉴于 GDPR 仅实施不到一年，很多工作仍有待完成，以改进程序、提高效率。对于一站式机制，由于在一站式机制下的案件数量和规模相对不大，尚未出现纠纷，因此 EDPB 还未行使过争议解决职能。对于一致性机制，EDPB 发布的意见主要集中在数据保护影响评估处理主体名单上，在其他领域发挥的一致性作用有限。未来 EDPB 计划对约束性公司规则、行为准则、标准合同、认证机制等问题作出澄清，以将一致性机制的作用拓展到其他领域。从各国监管机构年报也看的出其于 EDPB 之间保持着紧密联系与合作，例如对指南、意见等文件的制定和起草提供材料与建议。不过，一致性机制的开展比较消耗资源与时

间，其要求各机构能够在短时间内完成各种转化，因此更多文件的出台需要更长的时间。

在各监管机构的执法效果方面，一方面随着 GDPR 的生效，各监管机构的执法活动明显增多，执法力度也有所增强，另一方面，执法的实际效果仍有待观察和证实。

GDPR 的生效使得许多监管机构实现了权力的扩张和身份的转变，与以往被动的执法模式不同，后 GDPR 时代的监管机构倾向于积极主动的履行监管职能监督其管辖范围内机构的数据保护情况，即使尚未出现数据泄露等安全隐患。从现有执法活动来看，虽然各监管机构对大型科技公司显示出重点关注，中小型公司也未逃过其法眼。各监管机构不仅增加了罚款处罚的数量和数额，也积极利用矫正权，而后者对企业经营与品牌的影响甚至比前者更大。此外，从企业数据保护官（Data Protection Officer）人数的增加以及各监管机构受理个人投诉数量的大规模增加可以看出，GDPR 在现实中提高了企业与个人对数据保护合规意识。

GDPR 执法活动对于数据主体权利的保护和各大企业数据合规的影响也存在质疑之声。正如欧洲著名数据权利非盈利组织 NOYB 发起人 Max Schrems 所指出，2000 万欧元或上一年全球总营业额 4%的罚款对不同企业的威慑效果不同，尽管 GDPR 列明了罚款的考量因素，实践中也很难作出合理且有效的罚款处罚。再者，对 GDPR 所详尽规定的基础权利和义务的实际遵守效果也很难证实。此外，尽管有 EDPB 的协调和监督，鉴于各国执法路径与社会文化的不同，欧洲各国的数据保护执法水平不均衡的现状短期内很难得到较大改善。

二、GDPR 合规体系

（一）风险评估

风险评估贯穿于企业 GDPR 合规制度的建立、实施以及更新完善的每一步，也是企业判断 GDPR 合规制度是否必要以及如何建设的首要步骤。合规初期，企业进行 GDPR 风险评估的重点主要为：（1）GDPR 是否适用；（2）GDPR 所涉及的业务领域及其数据的收集、使用、处理、保存和跨境传输的状态。

1. GDPR 是否适用？

GDPR 对于适用范围的界定采用的是影响主义原则，使得 GDPR 具有一定程度的域外适用效力而并不仅仅局限于欧盟境内，因此，即使是欧盟境外的企业也可能面临 GDPR 合规风险。从企业的角度而言，进行 GDPR 合规风险评估所要面临的首要问题在于确定自身是否应当受到 GDPR 的监管。

具体而言，根据 GDPR 第 3 条的规定，GDPR 不仅适用于设立在欧盟境内的数据控制者或处理者，还适用于设立在欧盟境外但向欧盟境内的数据主体提供商品/服务、或监控欧盟境内数据主体的行为的数据控制者或处理者。因此，企业在判断自身是否属于 GDPR 监管对象时，可以比照如下问题逐项进行筛查，以确定是否应当受到 GDPR 的规制：

（1）企业是否系设立于欧盟境内的数据控制者或处理者

GDPR 规定，若企业属于设立于欧盟境内的数据控制者或处理者，则无论其数据处理的具体行为是发生在欧盟境内还是境外，只要个人数据处理活动发生在该企业开展活动的场景中，即会受到 GDPR 的规制。企业可参照下列问题逐步判断其是否系设立于欧盟境内的数据控制者或处理者：

1）企业是否属于数据控制者或处理者？

GDPR 在第 4 条中对数据控制者和数据处理者进行了定义。具体而言，数据控制者是指能够单独或联合决定个人数据的处理目的和方式的自然人、法人、公共机构、代理机构或其他组织。例如，用户在某购物网站消费，如购物网站在此过程中获得了一定的用户消费数据，并能够决定这些数据的处理目的和方式，则很有可能被认定为数据控制者。

数据处理者是指为控制者处理个人数据的自然人、法人、公共机构、代理机构或其他组织。GDPR 项下所定义的数据处理的范畴非常广泛，包括对数据进行收集、记录、组织、建构、存储、修改、检索、咨询、使用、披露等自动化或非自动化单个或一系列操作。同样以购物网站为例，网站获得用户消费数据后，如决定与数据公司合作，由数据公司协助其进行用户数据分析和偏好预测，则该数据公司则很有可能被认定为数据处理者。同样，如果该购物网站与某云服务提供商合作，利用该云服务存储前述消费者数据，则该云服务提供商业也可能被认定为数据处理者。

2）企业是否设立在欧盟境内

欧盟境内注册成立的数据控制者或处理者毫无疑问属于设立在欧盟境内的企业的范畴。对于在欧盟境外注册成立的数据控制者或处理者而言，对这一问题的判断主要是看其是否在欧盟境内设有实体机构，包括分公司、代表处等。GDPR 序言第 22 条对于是否存在实体机构的判断，并不拘泥于其具体的法律形式，核心判断要素在于“是否能够通过稳定的安排从而真实有效地开展活动”。如是，则企业很有可能会受到 GDPR 的规制。

3）企业是否发生了与欧盟境内设立机构所开展的活动场景实际相关的数据处理

如果上述符合条件的设立机构本身及其开展的活动并不涉及任何包括数据收集、记录、储存、使用等一系列数据处理活动，则其受到 GDPR 规制的可能性较低。反之，如果存在与设立机构开展活动所实际相关的数据处理，则无论该数据处理活动是否实际由该分支机构进行，也无论该数据处理是否发生在欧盟境内，则企业均有可能会受到 GDPR 的规制。例如，中国某服装企业在欧盟境内设有分支机构，负责在欧盟境内的销售活动，并同时负责收集欧盟境内的消费数据，但会将收集来的消费数据定期回传至中国总部进行处理，则该企业很有可能会受到 GDPR 的规制从而需要履行 GDPR 所规定的相关义务。

（2）非设立在欧盟境内的数据控制者或处理者的数据处理是否受到 GDPR 规制

GDPR 规定，即使数据控制者或处理者并未设立在欧盟境内，但如果其数据处理行为与其欧盟境内的数据主体提供商品/服务或者监控欧盟境内数据主体的行为有关，则也应当受到 GDPR 的规制。对于并非设立在欧盟境内的数据控制者或处理者而言，可以参照以下问题逐步判断其是否受到 GDPR 的规制：

1）数据处理是否与其向欧盟境内的数据主体提供商品或服务相关？

从非设立在欧盟境内的数据控制者或处理者的角度而言，企业重点应该关注其线上网站是否向欧盟境内的数据主体提供商品或服务。实践中较为常用的判断标准包括企业的网站是否使用欧盟成员国所使用的语言、是否接受欧元作为计量/结算货币、线下配送范围是否及于欧盟境内等。企业也可以通过内部销售或服务记录来判断是否实际存在向欧盟境内的数据主体提供商品或服务的情形。

例如，在中国境内注册成立的公司运营某电商平台，并通过电商平台的运营获得大量用户消费数据，由于该公司在欧盟并未设立分支机构，因而并不属于设立在欧盟境内的数据控制者或处理者。但是，如果该电商平台的网站提供德文版本的页面，接受欧元作为结算货币进行结算，提供向欧盟境内的配送服务，则很有可能被认定为向欧盟境内数据主体提供商品或服务的数据控制者或处理者，从而受到 GDPR 的规制。

2）数据处理是否与其监控欧盟境内数据主体在欧盟境内的行为相关

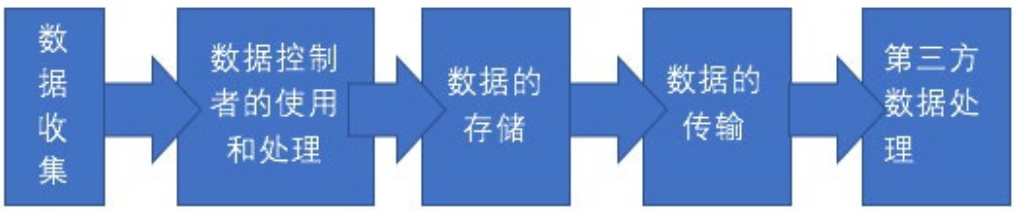
如果在欧盟境外设立的企业发现其所流入数据中有来源于欧盟的数据，则可能其在业务开展的过程中存在对于欧盟境内数据主体在欧盟境内行为的监控，从而很有可能会受到 GDPR 的规制。

例如，欧盟公民在我国旅游期间购买了 A 公司所生产的智能手机，A 公司会通过该智能手机对用户进行使用的过程中的使用数据进行收集。在该欧盟公民返回欧盟境内之后，继续使用该智能手机，A 公司也并未停止对于该部手机所产生的数据的收集。这一情形下，虽然 A 公司在欧盟境内并未开展任何经营，也很有可能会受到 GDPR 的规制。

2. GDPR 所涉业务领域筛查及其数据生命周期分析

在企业经过初步判断确定属于 GDPR 的规制范围之后，则需要更进一步地对企业自身的业务活动和领域进行梳理和筛查，并对相关数据的收集、使用、处理、保存和跨境传输的状态进行具体的梳理和分析。在实践中，为了保证全面、准确地识别企业可能受到 GDPR 影响的具体业务领域和数据处理活动， 通常建议企业首先按照自身主要经营活动为模块进行梳理和筛查， 确定 GDPR 合规风险较大的业务模块和领域。其次，在确定主要涉及 GDPR 合规的业务领域之后，企业可以根据每个业务模块的具体业务流程，按照所涉及到的数据收集、使用、处理、保存和跨境传输等数据处理周期中的具体环节，比照 GDPR 中所规定的

数据处理的基本原则、数据处理活动中数据主体的权利以及数据控制者和处理者的义务，识别企业所进行的数据处理周期中每一环节所可能存在的风险和问题，从而锁定出不同业务中 GDPR 合规风险较大的具体数据处理环节。



具体而言，企业可对其数据处理周期中的每个环节作如下梳理：

（1）数据收集

数据收集是企业进行数据处理活动的起始环节。企业在对特定领域业务中涉及到数据收集的环节进行风险梳理时，可以重点比照 GDPR 中的下列要求，确定企业在特定目标业务领域中的数据收集环节是否存在较大的风险：

1）数据收集前是否进行充分告知

GDPR 中规定数据控制者或处理者在向数据主体进行数据收集前，需以清晰明确、易于理解的方式向数据主体告知有关数据收集和处理的相关信息，具体包括：

a. 数据控制者、数据处理者以及二者的数据保护官（DPO，如有）的身份和联系方式，如电话、电子邮箱、邮寄地址等；

b. 数据收集的目的、种类、数量、范围；

c. 数据收集后可能进行的数据处理活动；

d. 数据的存储期限；

e. 数据接收方或接收方的种类；

f. 数据主体所享有的主张数据获取、修改、删除、限制处理、反对处理、可携带等权利

除此之外，企业最好还能向数据主体披露：

a. 数据跨境传输的相关情况；

b. 所采取的安全保障措施的细节；

c. 向监管机构投诉的权利、个人数据的来源；
d. 撤回同意的方式等

2）数据收集前是否已获得同意

根据 GDPR 的相关规定，数据控制者或处理者向数据主体进行数据收集前，需在对数据主体进行上述告知的基础上，取得数据主体对数据收集的明示且自愿的同意，并告知数据主体其有权随时撤回同意。

3）数据收集是否具有其他合法事由

除前述数据主体的同意外，GDPR 还规定了其他五种数据收集和处理的合法事由，包括出于合同履行、履行法定义务、保护个人重要利益、维护公共利益以及追求正当利益的必要。企业可以参考这些合法事由的具体规定对自身的数据收集行为进行审查，保证其满足数据收集和处理的合法性要求。

（2）数据的使用和处理

企业可以重点比照 GDPR 中的下述要求，对目标业务领域相关数据使用和处理环节所涉及到的合规风险进行判断：

1）确保数据处理符合数据初始收集时的目的

GDPR 规定数据控制者或处理者所进行的数据处理应当符合初始收集时的目的。因此，建议企业在对目标业务领域的数据使用和处理环节进行核查时，注意比较其数据使用和处理的目的、范围、主体等内容相对于数据初始收集时是否发生变化；如发生变化，是否在使用和处理数据前对数据主体重新进行告知并取得数据主体合法有效的同意。

2）确保数据处理遵循准确、必要、及时的原则，并以相关、必要为限度

GDPR 规定数据控制者或处理者所进行的数据处理应当遵循准确、必要、及时的原则，并以相关、必要为限度。因此，建议企业在对目标业务领域的数据使用和处理环节进行核查时，注意判断其所进行的数据处理与数据收集的目的是否具有一定的相关性，是否在数据收集后的一定时间内发生以及是否为实现数据收集时的目的所必要。

3）确保数据主体能够限制数据处理

GDPR 明确数据主体有权限制数据控制者或处理者对其数据的处理活动。因此，建议企业注意核查其是否已经建立特定的机制或为数据主体提供特定的途径，以确保数据主体在特定情形（如当数据主体质疑数据准确性时，或数据处理系非法且数据主体反对删除数据时等）下可以限制数据控制者对自身数据进行处理的权利。

4）确保数据主体能够反对特定的数据处理

GDPR 明确数据主体有权反对数据控制者或处理者的特定数据处理活动。因此，建议企业注意核查其是否已经建立特定的机制或为数据主体提供特定的途径，以确保数据主体在特定情形下有权反对对其进行的特定的数据处理活动，包括以直接营销为目的的数据处理、数据画像等。

（3）数据的存储

GDPR 规定数据控制者和处理者对于能够识别数据主体个人数据的保存时限不得超过数据处理目的的必要。因此，建议企业注意核查其是否已经建立特定的机制或为数据主体提供特定的途径，以确保企业能够识别由于数据处理目的已经满足而存储到期的数据，并及时对到期数据进行删除。

（4）数据的传输

GDPR 规定数据控制者或处理者对数据主体数据的传输应当在采取特定的保护措施保障数据安全的情况下方可进行。此外，在技术可行的情况下，GDPR 规定数据主体有权要求将其个人数据从企业转移到另一个控制者手里且企业不应加以阻挠。因此，建议企业注意核查其是否已经建立特定的机制或为数据主体提供特定的途径，以确保数据主体能够进行上述数据传输。

（5）第三方数据处理

GDPR 规定数据控制者在选择数据处理的合作第三方时，应当选用具有充分保证的、采取合适技术与组织措施的、处理方式符合本条例要求并且能够保障数据主体权利的处理者。数据控制者应当在与第三方处理者的合同文本中纳入关于数据处理者 GDPR 合规义务的约定，这类合同和约定应当包括处理者相对于控制者的责任、主体事项、处理期限、处理性质与目的、个人数据的类型、数据主体的类型及控制者责任与权利等。因此，建议企业注意对已经开展合作以及所要进行合作的数据处理者及双方之间所订立或将要订立的文本进行仔细筛查，判断其是否符合前述要求。

在上述梳理工作完成之后，企业应当根据具体的识别结果形成企业内部的 GDPR 风险识别清单。企业可以该清单作为指导，结合 GDPR 的各项具体要求开展后续的具体合规工作。

（二）组织架构保障

为建立行之有效的 GDPR 合规制度，企业除进行前述风险评估并确定自身所面临的 GDPR 合规风险之外，还需要在组织架构上为合规制度的实施提供从上到下、全面覆盖、内外结合的全方位保障。

1. 管理层对数据合规的重视与支持

管理层的了解、认可和支持对企业内部有效建立 GDPR 合规制度至关重要。首先，由于管理层负责公司的日常经营和决策以及重要政策的制定，因而其本身对于 GDPR 的了解和重视是企业从整体上进行 GDPR 风险防范的重要一环。其次，管理层能够为企业的 GDPR 合规工作提供具体的资源和支持，例如提供资料获取的途径、专职的合规人员或聘请外部顾问、财务与预算的保障等，并且有助于通过制度约束等形式保证各部门的协调与配合。最后，管理层对于 GDPR 风险合规的支持，有利于向企业上下释放明确的信号，促进企业内部的各个部门及其人员之间就 GDPR 风险合规的重要性达成共识，从而有利于企业 GDPR 合规制度的整体建设和具体实施。

（1）董事会

对于存在 GDPR 合规风险的企业而言，董事会及其成员充分了解企业所面临的 GDPR 合规风险，有利于将 GDPR 合规风险的管控纳入企业的重大合规事项管理体系，推进 GDPR 合规方案的落实与推进。为实现这一目的，企业可以：

1）在合规委员会下设数据合规小组。如企业设有合规委员会，则合规委员会在处理数据相关问题时，可建立数据合规小组，由涉及数据处理的业务部门人员以及专门负责 GDPR 合规的合规人员及企业内设的 DPO 等组成，负责企业的数据合规风险管控。

2）合规委员会与合规小组负责人定期会谈。合规委员会可定期与 GDPR 合规主管负责人员进行会谈，或听取相关负责人就企业日常经营中存在的 GDPR 合规问题的汇报，了解企业在各项业务中所面临的 GDPR 合规风险及可能采取的应对措施；

3）重大事项提请董事会讨论。合规委员会可在董事会对公司经营的重大事项尤其是可能存在 GDPR 合规风险的事项进行决策的过程中，就数据合规人员的意见提请董事会，确保董事会有机会对可能涉及的 GDPR 合规风险进行充分考量。

4）任命数据合规管理人员并保障其独立性。董事会在任命企业的高级管理人员以及进行管理层设置之时，应尽可能充分听取合规委员会的意见，结合企业实际情况，任命专职或兼职的数据合规管理人员担任较高职位，确保其独立性，并赋予其履行职责所必须的职权、资源以及人员配备。

（2）高管人员

建议企业根据 GDPR 合规活动的实际需要，在核心高管人员中设专职或兼职负责 GDPR 合规的人员，负责公司整体上的 GDPR 合规运营工作，并赋予其能够直接向董事会进行汇报的权力。此外，建议企业的高管人员之间可定期召开以 GDPR 合规为主题的业务交流会议，就业务中所可能存在或已经出现的数据保护风险开展讨论和交流。

（3）合规问责制度

建议企业结合具体的业务情况，制定具体的 GDPR 合规问责制度。企业可将员工对企业内部 GDPR 合规制度的遵守情况纳入到员工考评中，具体可归入合规情况考核项下，并与员工的奖惩挂钩。同时，建议企业根据 GDPR 的具体要求，制定具体合规政策，明确不同部门的负责人员，确保在发生违反 GDPR 合规要求的事件发生之后，能够及时采取措施进行补救，并追究违规人员的责任。

2. 是否需要设置 DPO？

（1）DPO 的设置、选任及其职责范围

GDPR 第 37 条规定了数据控制者和数据处理者应当任命 DPO 的情形，包括：（1）公权力部门或机构进行数据处理活动的；（2）数据处理的核心活动涉及对数据主体进行经常性大规模系统化监控的；（3）特殊类别个人数据或与刑事违法行为相关的个人数据的大规模处理。

除上述情形之外，GDPR 并未要求企业设置 DPO。尽管如此，我们仍然建议企业在可行的情况下尽可能设置 DPO，根据企业实际的 GDPR 合规需求，灵活安排企业内部人员全职或兼职担任。这是因为，企业 DPO 的设立不仅是企业

完善的内部合规制度的有力证明，而且有利于企业后续具体 GDPR 合规工作的开展，能够为企业提供具体的合规指导。有关 DPO 的具体设置、选任及其职责范围的详细介绍，请参见第三章之如何设定 DPO 的部分。

（2） DPO 与现有组织架构的衔接和整合

企业 DPO 的设置是否能够为企业 GDPR 合规提供有效的保障，在一定程度上取决于 DPO 是否能够与企业现有组织架构进行衔接和整合。因此，建议企业在考虑对 DPO 进行设置时，充分利用和整合企业内部现有资源，确保 DPO 以高效的方式履行 GDPR 项下的职责。

1）整合企业内部现有的合规资源

建议企业在设置 DPO 之前，对内部现有处理数据合规相关事宜的人员、资源及制度进行梳理，并结合企业 GDPR 具体合规需求，确定是否可由现有合规人员兼任 DPO 或为 DPO 提供人员支持，以判断是否可在现有的合规制度的基础上进行增改而构建 GDPR 合规制度。

2）识别并避免与现有组织架构间的利益冲突

DPO 承担着对企业数据处理活动合规情况的监督职责，其职责的履行应具备较强的独立性。因此，建议企业在设置 DPO 之前，对现有组织架构进行简单分析，识别现有组织架构中可能与 DPO 及其辅助人员职责存在利益冲突的人员及岗位，确保 DPO 及其辅助人员不应由与数据处理活动有关的人员担任，最大限度地保障 DPO 职责的履行。

3）保障 DPO 与现有组织架构间的独立性

确保 DPO 人事上的独立性。为了保障 DPO 履行职责所需要的独立性，建议企业在现有组织架构中设置 DPO 时，还要确保 DPO 在人事关系上独立于从事数据处理活动的相关人员，并赋予 DPO 直接向董事会进行汇报的权力，保障 DPO 在企业数据相关问题上能够形成独立的判断而不受他人影响。

DPO 不应当因履行职责而受到惩戒。根据 GDPR 的规定，数据控制者或处理者不得因为 DPO 履行其职责而对其实施惩戒。因此，建议企业在设置 DPO 时对此进行制度化明确。

4）构建 DPO 对业务活动的参与机制

企业可以建立明确的 DPO 对业务活动的内部参与机制，针对企业与 GDPR 相关的业务，赋予 DPO 履行职责的具体权力，并规定企业相关部门的配合义务，确保 DPO 能够对企业上下的 GDPR 合规情况进行有效监督。具体如下：

a.建议企业及企业的业务部门定期邀请 DPO 参加业务会议，促进 DPO 对于企业业务和基本情况的了解；

b.建议企业从设计着手保护隐私（Privacy by Design），即从产品或服务开发前期开始就应保障数据合规团队及人员与开发和设计团队相互合作，从产品设计伊始即对产品及产品相关文本中所涉及到的数据保护问题进行考量；

c.建议企业明确其他部门在涉及数据保护的相关问题时向 DPO 进行告知的义务，确保 DPO 能及时了解企业的数据保护问题；

d.建议企业在数据泄露事件或其他数据问题事件发生时向 DPO 进行咨询，听从 DPO 的处理建议；

e.建议企业规定 DPO 对数据问题的建议或意见应当被相关业务人员听取并遵守，如果相关业务人员拒绝听取 DPO 的意见和建议，则应当书面记录拒绝理由；

f.建议企业规定相关业务人员未就数据问题向 DPO 咨询或未遵守 DPO 的建议或意见即作出决策或采取行动，DPO 表示反对的，应当将 DPO 的反对意见进行书面记录。

（3）其他管理资源配置

不同的企业在进行 GDPR 合规制度的构建过程中，由于所面临的实际风险和所能调动的合规资源存在差异，企业往往需要结合自身的实际情况作出符合自身实际情况的制度安排。

1）主营业地管理资源配置

如前所述，GDPR 规定了一站式监管机制，即企业的主营业地（主要涉及数据处理活动的营业地）所在国的监管部门是企业的主监管机关，企业通常并不需要应对欧盟境内其他国家的监管机关。因此，在企业合规资源有限的情况下，我们建议企业将 GDPR 合规的主要人员和资源重点分配在主营业地。

2）根据风险识别进行管理资源配置

从业务角度而言，在企业合规资源较为有限或 GDPR 所涉业务较窄的情况下，建议企业在完成企业内部 GDPR 风险的识别之后，根据风险识别的结果，

将存在较大 GDPR 合规风险的业务领域和业务单元作为管理人员和管理资源的分配的重点领域。

3）欧盟境内代表的设立

根据 GDPR 的规定，对于非在欧盟境内设立但是因处理欧盟境内数据主体的数据或对欧盟境内数据主体持续监控而受到 GDPR 规制的数据控制者或处理者，除涉及特殊数据的处理或系公共机构或团体等特殊情形外，应当以书面方式指定一名在欧盟的代表。该代表应当设立在接受商品或服务，或者行为受到监控的数据主体所在成员国。数据控制者或数据处理者所指定的代表在开展活动时，应当得到数据控制者或数据处理者的授权，同时也需取得监管机构和数据主体的授权。

（三）合规体系设立与执行

企业实施 GDPR 合规业务，除进行整体合规风险的评估以及组织架构的搭建之外，更为关键的是如何在企业的具体事项上落实 GDPR 的具体要求。因此，我们建议，企业应当设立一套较为具体的 GDPR 合规标准，以供内部统一参照执行。

1. GDPR 合规制度的设立与健全

企业内部 GDPR 合规制度的建立，除了需要帮助企业厘清在 GDPR 项下可能存在的风险，并从组织架构方面搭建企业内部 GDPR 合规框架之外，还需要在微观上就内部履行对 GDPR 项下所规定的各项具体义务为企业上下提供具体的参考标准，构建具体的行为机制，从而使企业的 GDPR 合规制度逐步健全与完整。

1）保障个人数据主体的权利

GDPR 不仅整章的篇幅规定了数据主体所拥有的广泛权利，作为呼应，还规定了数据控制者和处理者采取技术性措施或组织性措施保护数据主体权利的义务，并针对未履行相关义务的行为规定了相应处罚。因此，对于企业而言，在 GDPR 的内部合规标准中明确企业保障 GDPR 项下数据主体各项权利的具体机制至关重要。具体而言，企业应当为数据主体实现以下权利提供保障：

a.获取自身数据的权利

企业应保障数据主体可随时要求企业提供其个人数据，获得自己的数据副本。数据主体向企业请求获得与数据处理相关的个人数据的，企业应当以透明、清晰且易于获取的方式、且应当自收到请求后不超过 1 个月（复杂情况下至多不超过 2 个月）向数据主体提供所请求的个人数据。如果未根据请求采取行动，企业应当自收到请求之日起不超过 1 个月通知数据主体未提供其个人数据的原因，以及向监管机构申诉和寻求司法救济的可能性。

b. 数据收集前的知情权

企业从数据主体处收集个人数据，应当向数据主体提供以下信息：（a）控制者的身份和联系方式；（b）DPO 的联系方式；（c）控制者或第三方所追求的合法利益；（d）数据接收方或接收方类型；（e）个人数据的存储期限；（f）数据主体所享有的数据获取、修改、删除、限制处理、反对处理、可携带等权利；（g）数据主体所享有的撤回同意的权利；（h）数据主体所享有的向监管机构申诉的权利；（i）自动决策机制，包括数据画像以及有关的逻辑程序和有意义的信息，以及此类处理对数据主体的意义和预期影响。

c. 数据访问权

企业应当采取措施保障数据主体有权从控制者处确认自己的个人数据是否正在被处理，并可以访问个人数据；企业应保障用户有权查询自己的个人数据、处理目的、个人数据的类别、接收者、存储期限、自动决策机制、传输到第三国的有关保障等信息。

d. 更正权

企业应当保障用户可随时要求企业更改自己错误、不准确、不完整的数据。

e. 删除权

企业应当采取措施保障数据主体可随时要求企业删除自己的个人数据。除为言论自由、公共利益等必要，在下列情形下企业应当满足数据主体要求删除相应数据的主张：（a）就收集和处理数据的目的而言，该数据已非必要；（b）数据主体撤回同意，且控制者不存在其他个人数据处理的合法依据；（c）数据主体反对处理，且控制者不存在其他个人数据处理的合法依据；（d）个人数据被非法处理的。

f. 限制数据处理权

在下列情形下，企业应当采取措施保障数据主体可以限制企业对其个人数据进行处理的权利：（a）数据主体质疑数据准确性，且允许企业在一定期限内核实；（b）该处理是非法的，但数据主体反对删除数据；（c）企业不再需要数据但是数据主体为法定请求权的确立需要该数据的；（d）数据主体反对数据处理，但需要核实企业的法律依据是否优先于数据主体的。

g. 数据可携带权

企业应当在技术可行的前提下，采取措施保障数据主体能够以结构化、通用的机器可读方式，将其个人数据从企业转移到其他数据控制者且不受阻挠的权利，除非为公共利益的目的或者对其他主体的权利和自由产生不利影响。

h. 反对数据处理的权利

企业应当采取措施保障数据主体有权反对对其个人数据进行处理，包括以直接营销为目的的数据处理、数据画像等，数据主体有权对这些处理提出反对并要求不受这些处理行为的限制。

2）保障个人数据生命周期的安全

根据 GDPR 的规定，企业在涉及到数据收集、使用、处理、保存和跨境传输的整个数据生命周期，均应当保障数据主体的个人数据安全。因此，企业应当基于风险评估所确定的不同业务中 GDPR 合规风险较大的具体数据处理环节，根据前文中所涉及各环节应当履行的义务和遵守的程序，设立具体的行为机制，以确保数据主体个人数据生命周期的安全。

3）建立和实施个人数据保护影响评估机制

a.个人数据保护影响评估（DPIA）

GDPR 规定数据控制者应当在进行特定的数据处理之前进行个人数据保护影响评估，尤其是当数据处理的行为涉及自动化决策领域、大规模特殊种类的数据处理以及公共领域的大规模系统性监控等情形时。

个人数据保护影响评估能够帮助企业识别并应对潜在风险，并帮助企业满足 GDPR 项下的要求，对于企业而言具有重要意义。因此，建议企业在 GDPR 内部

合规标准中设立实施个人数据保护影响评估的具体机制，明确在上述情形下实施个人数据保护影响评估的具体要求，并确保该机制能够符合下列要求：

a. 系统性地描述数据处理的目的；
b. 对处理操作的必要性和适当性进行评估；
c. 对数据主体的权利和自由的可能影响或造成的风险进行评估；
d. 对将采取的保障措施和安全机制是否符合 GDPR 要求进行评估；

此外，企业最好能够明确规定特定情形下个人数据保护影响评估后如何与监管机构进行咨询的具体机制。根据 GDPR 的规定，如果数据保护影响评估的内容表明数据处理将会给数据主体的个人数据安全带来较高风险，则控制者应当在进行数据处理之前与监管机构进行协商和咨询。

b．如何进行 DPIA

对企业而言，DPIA 是一种系统地全面分析企业的个人数据处理过程，帮助企业识别并最小化数据处理风险的方法。DPIA 应考虑合规风险，但也应考虑对个人权利和自由的更广泛风险，包括潜在的任何重大社会或经济问题。其重点是对个人或整个社会造成的潜在伤害。

如前所述，在开始“可能导致高风险”的任何类型的个人数据处理之前，企业必须进行 DPIA。这意味着，虽然企业尚未评估实际风险等级，但需要筛查出可能对个人造成广泛或严重影响的因素。

GDPR 尤其指出，企业如果计划进行下列事项，则必须进行 DPIA：

- 使用系统性的、广泛的、具有重要影响的用户画像
- 大规模地处理特殊类型或刑事犯罪数据；或
- 大规模、系统性地监视可公开进入的场所。

DPIA 应当开始于项目生命周期的早期，在开始处理个人数据之前，并与规划和开发过程同步延续进行。具体而言，DPIA 应该包括这些步骤：

- 识别进行 DPIA 的需求
- 对个人数据处理进行描述
- 对咨询方面进行考虑
- 评估数据访问的“必要性”与“适当性”
- 识别并评估风险

- 识别降低风险的措施
- 确认并记录结果
- 将结果整合至行动中
- 持续审查

4）管控数据处理者的数据合规风险

GDPR 对于数据控制者选择开展合作的数据处理者的行为赋予了一定的审慎义务，并规定数据控制者对于数据处理者的行为负责，从而间接实现了对数据处理者义务的施加。这就决定了作为数据控制者的企业对开展合作的数据处理者的 GDPR 合规风险管控，也是其自身进行 GDPR 合规的重要部分。

因此，建议作为数据控制者的企业在 GDPR 的内部合规标准中建立一套具体的审查机制。该机制应当确保：

（a）建议企业选用能够就数据安全提供充分保证的、可采取合适技术与组织措施的、处理方式符合 GDPR 要求且有能力保障数据主体权利的数据处理者；

（b）建议企业在与数据处理者所签订的数据处理合同中对处理者进行约束，确保该合同规定：a）处理的内容和期限；b）处理的性质和目的； c）个人数据的类型和数据主体的类别；d）数据处理者的义务。

5）个人数据出境

根据 GDPR 的要求，企业对于正在处理或计划进行处理的个人数据，将其转移到第三国或国际组织、从第三国或国际组织转移到另一第三国或国际组织，必须确保该第三国或国际组织系经欧盟委员会认定可以提供充分保护的第三国或国际组织。如缺乏上述充分保护水平，企业仅能在提供了 GDPR 下所要求的适当保障并且已经提供数据主体权利和救济的情况下将数据主体的数据转移至向第三国或国际组织。前述适当保障包括 GDPR 第 47 条中所述有约束力的公司规则、经欧盟委员会批准的标准数据保护条款等。

因此，如果企业的数据处理中可能涉及个人数据出境，建议企业在 GDPR 内部合规标准中就企业所掌握或处理的个人数据的出境所应遵循的标准进行具体性规定。

6）个人数据泄露的处理机制

GDPR 规定了数据控制者或数据处理者企业在发生个人数据泄露时的相应义务。因此我们建议，企业所制定的 GDPR 内部合规标准中应当包括个人数据发生泄露时的处理机制，从而确保数据泄露事件对个人数据安全影响的最小化。上述处理机制应当至少保证以下事项：

a. 个人数据处理者在发生数据泄露后立即通知数据控制者，而无需对数据泄露事件可能的风险进行评估；

b. 数据控制者应当在知晓数据泄露事件后 72 小时内向监管机构进行报告，未能在 72 小时内进行通知的，应当对迟延理由加以说明。

c. 数据控制者向监管机构进行的报告应当明确泄露涉及的个人数据的种类、数量、DPO（如有）的姓名及联系方式、泄露可能导致的后果以及已经或可能采取的补救措施等，从而识别数据泄露可能引发的特定损害风险。

d. 若数据的泄露可能给自然人的权利与自由带来高风险时，控制者应当及时（例如在 72 小时内）将泄露告知数据主体，例如，提供在线服务的数据控制者因网络攻击导致个人数据泄露、数据控制者遭受勒索软件攻击而导致所有数据被加密并且没有备份等。除非：（a）控制者已经对被泄露数据采取适当的技术性和组织性保障措施；（b）控制者已采取措施确保该类高风险情形不会再出现；（c）进行告知需要不成比例的工作量。

e. 数据控制者应当完整记录泄露的情况，包括泄露事件的原因、受影响的数据主体、影响和后果、补救措施等。

7）数据处理操作记录

GDPR 规定了员工规模达到 250 人及以上的数据控制者和数据处理者应当对其数据处理操作制作登记册加以记录，包含相关处理操作的具体信息。应监管机关的相应要求，数据控制者、数据处理者还应当向监管机关提供该登记册。因此，建议企业在内部的 GDPR 合规标准中也建立相应的记录机制，以确保：

a. 作为数据控制者的企业应当就其进行的数据处理活动进行记录，记录内容至少包括：（a）控制者及控制者的代表、DPO 等的姓名及联系方式；（b）数据处理的目的；（c）对数据主体类型及个人数据类型的描述；（d）对个人数据接受者类型的描述；（e）个人数据转移到第三国或国际组织的记录，及采取的保障措施的记录；（f）技术性与组织性安全措施的一般性描述等。

b. 作为数据处理者的企业应当就其以控制者名义进行的数据处理活动保存一份记录，记录内容至少包括：（a）处理者或处理者们的名字和详细联系方式、

处理者所代表的每个控制者或处理者的代表、DPO；（b）代表每个控制者进行处理的类型；（c）将个人数据转移到第三国或国际组织的记录，以及采取的保障措施的记录；（d）技术性与组织性安全措施的一般性描述等。

8）处理个人数据的内部工作人员的保密义务

GDPR 对于被授权处理个人数据的工作人员（例如企业内部的商业部门和人力资源部门等）规定了特定的保密义务。因此，建议企业应当根据自身的实际需要起草对处理个人数据的工作人员的保密制度规定，并与涉及到对个人数据进行处理的员工签订保密协议或订立保密条款，确保处理人员对于所处理数据及对应的处理活动保密。

2. GDPR 项下外部文本的调整与完善

在明确了企业在 GDPR 项下各项义务的具体合规标准及行为机制并加以实施的基础上，建议企业结合具体的合规标准及行为机制，对企业与第三方之间的文本进行深入梳理，对其中可能与 GDPR 相关的文本相应进行调整与完善，从而能够保证企业在外部文本层面的合法合规性。

1）隐私声明与通知

GDPR 提高了企业在进行个人数据收集前的透明度要求。如前所述，根据 GDPR 的规定，企业在对数据主体的个人数据进行收集之前，应当向数据主体提供包括收集性质、种类、目的、期限等在内的一系列信息，并取得数据主体的同意。同时，如果被收集个人数据的对象系企业雇员，则企业相应地也需要保障雇员就其个人数据被收集和使用的情况保持知情和同意。

在实践中，我们建议企业在产品或服务的隐私声明或雇员隐私通知中向用户或雇员进行以上告知，以实现上述目的，具体而言，建议企业建立以下操作机制：

a. 确定网站、APP、售后服务电话中心、人力资源管理中心等不同部门需要进行的数据处理活动；

b. 进一步确定需要通知数据主体的数据处理活动内容及其需要收集相关数据，示例：“为保障你正常使用我们的服务，我们会收集你的设备型号、操作系统、唯一设备标识符、登陆 IP 地址、软件版本号、接入网络的方式和类型、设备加速器（如重力感应设备）、操作日志等日志信息，这类信息是为提供服务必须收集的基础信息。”

c. 结合上述基础，起草网站、APP、售后服务电话中心、人力资源管理中心等不同部门的隐私政策声明；

d. 确保上述隐私政策声明以合理可见的方式传达至相应的数据主体，例如，可以通过确认协议、具体场景下的文案确认动作等形式进行；

e. 确保在隐私政策声明的设计下，同意仅在数据主体以明示、自愿、清晰的方式作出时方为有效，例如，将隐私政策声明植入在网站或应用页面的显著位置，或以弹窗的形式给予数据主体提示，并需要数据主体进行明确勾选动作。此外，当用户不同意企业的隐私政策声明时，企业对用户使用服务的限制应尽可能地在合理必要的范围之内。示例："请注意，为确保会员身份真实性、向您提供更好的安全保障，您可以向我们提供身份证、军官证、护照、驾驶证、社保卡、居住证等身份信息、面部特征等生物识别信息…完成实名认证。如您拒绝提供上述信息，可能无法使用账户管理、创建店铺、出售商品、继续可能存在风险的交易等服务，但不会影响您使用浏览、搜索等服务"。

2）与第三方之间的数据处理协议

如前所述，GDPR 中规定数据控制者在与数据处理者（譬如薪酬服务提供商、人力资源平台商和云服务等）进行合作时，数据处理者必须受到符合 GDPR 要求的协议约束。协议的内容应当包括：a）数据处理的内容和期限；b）数据处理的性质和目的； c）个人数据的类型和数据主体的类别；d）数据处理者的义务等。此外，出于对数据主体个人数据的保护，数据控制者在与第三方签订的数据处理协议中，应当以保密条款的形式，清晰明确地约定第三方的保密义务。因此，建议作为数据控制者的企业确保企业与满足合作条件的数据处理者订立的协议尽可能地包含上述内容。

3）数据跨境传输的合同保障

GDPR 限制个人数据向欧洲经济区以外的国家或国际组织转移，除非第三国或国际组织被认为提供了充分的保护水平或者提供了适当的保障及权利保护和救济。由于我国并不未通过欧盟委员会数据保护充分性认证，因此，除非作为数据控制者的企业可以提供 GDPR 所要求的适当的保障及权利保护和救济，否则不允许其将欧盟境内的个人数据转移到国内。这里的转移既包括实际转移（如发送 Excel 表格）也包括提供对欧盟经济区中的服务器的远程访问。这些限制也适用于同一集团企业内部各公司之间的转移（如从欧盟境内的公司到中国的公司）或向服务提供商转移。

GDPR 项下的适当保障包括有约束力的公司规则、公共机构或实体之间订立的具有法律约束力并可执行性的文件，经欧委会批准的标准数据保护条款等。因此，我们建议企业在涉及到对个人数据跨境传输时，应当根据 GDPR 相关规定，在合作协议之外增加符合 GDPR 相关规定所具体要求的规则、协议或文件，以确保数据跨境传输的合规进行。

3. GDPR 合规的流程管控

对于涉及大量 GDPR 合规工作的企业而言，针对 GDPR 具体合规标准的建设，可能会涉及到多个上述具体合规行为机制的确立和实践，如不进行适当的流程管控，则既可能会存在彼此割裂、效率不高的情况，又可能会出现相互混淆、管理混乱的情形。因此，建议企业就上述各个具体行为机制单独制定各自的行为规则和流程，但在实际进行履行和合规流程管控时，仍然按照业务模块并以数据处理的生命周期作为逻辑主线，分块分段进行合规实践，并在每一个块和段上综合运用上述各个行为机制和标准。

（四）合规培训及宣讲

定期对企业的董事、高管、雇员和第三方开展多元化的 GDPR 培训是企业进行有效的 GDPR 合规的重要环节，也是监管机构在评估企业内部 GDPR 合规制度有效性的主要关注点之一。我们建议，为使合规培训的作用实现最大化，企业可以针对不同的人员设置不同类型和层次的培训，构建细致而有所区分的培训机制。具体而言，建议企业可以着眼于以下几个方面展开 GDPR 的合规培训：

1. 管理层合规风险意识的提高与强化

管理层的合规风险和意识的提高与强化对于企业合规体系的构建有着重要的作用，它在很大程度上决定着企业上下对于合规的重视程度。管理层合规风险意识的提高与强化，管理层关于 GDPR 合规内容的了解，有利于将 GDPR 合规问题的考量贯彻到企业的日常运营以及决策考量的过程之中。因此，建议企业要求管理层定期与 DPO、 GDPR 合规人员进行沟通，由其定期组织针对管理层的 GDPR 合规培训，就企业内部有关 GDPR 的案例进行汇报和讨论，并定期向管理层推送 GDPR 的执法动态和相关立法与指引的制定情况，就企业 GDPR 风险合规的状况进行评估分析，提高管理层的合规风险意识。

2. 员工培训

企业员工直接从事企业的一线具体工作，因而是最有可能进行风险识别并进行控制的环节。因此，我们建议企业对于员工的 GDPR 培训给予充分的重视，定期举行针对员工的各类培训，并对员工培训中所涉及到的具体情况留存记录。从培训方式和类型上看，我们建议企业具体采用以下形式对员工进行培训：

1）一般性定期培训

建议企业定期邀请从事 GDPR 合规的专业人士为员工开展关于 GDPR 合规知识的普及性培训，确保员工了解 GDPR 的主要内容和影响，以及企业在 GDPR 项下所面临的主要风险。

2）专项业务培训

实践中，企业在具体业务上所面临的 GDPR 合规风险各有不同，仅仅进行一般性的定期培训可能无法充分有效地帮助业务人员在实际工作中识别 GDPR 项下的合规风险。因此，建议企业应当在前述定期培训的基础上，邀请具备专业人员，针对不同的核心业务模块组织不同主题的业务培训，并根据员工所从事的工作内容、性质、风险制定培训的内容和计划，就员工在具体业务工作中如何识别并控制 GDPR 风险提供具体指导。例如，针对售后服务中心、销售中心、人力资源管理等直接与用户或雇员接触并收集和处理数据的部门，围绕其涉及到的数据收集、处理、使用、存储等活动进行专门的业务培训设计。值得注意的是，对于核心业务岗位的工作人员所提供的培训，我们建议应当以现场培训为主。

3）线上培训

除了前述现场一般性定期培训和专门性业务培训之外，企业也可结合自身实际情况，定期召开远程培训或业务交流会议，开发企业内部的 GDPR 合规学习测试系统，定期上传 GDPR 有关的在线培训视频材料供员工学习，并组织对员工进行线上检测，及时巩固合规培训的结果。

3. 第三方培训

如前所述，GDPR 项下不仅对数据控制者的义务作出了规定，而且还规定了数据控制者应当选择满足 GDPR 要求的数据处理者进行合作，并对 GDPR 项下的数据处理者提出了对应所需要满足的义务。因此，第三方合规意识和能力的强弱也有可能对企业自身产生影响。因此，我们建议企业在进行合规机制设置时，

除了注重管理层和员工的培训，还应注重对第三方的培训。譬如，企业可以定期派出 GDPR 的专业合规人员去合作的第三方进行业务交流或举办讲座，提高第三方的合规风险意识和能力。

（五）合规体系执行的监督和审计

企业在构建起较为完善的内部 GDPR 合规制度之后，建议定期由企业的内部审计部门对合规制度的执行情况进行梳理，从而实现对合规执行情况的监督和审计，并就审计的结果形成审计报告。审计报告应当交由包括企业 GDPR 合规负责人在内的管理层人员进行审阅，并抄送企业 DPO（如有）。管理层审阅报告之后，可就审计结果与 DPO 进行合议，就审计结果中所涉及到的相关问题在企业内部进行通报，要求存在问题的业务部门根据审计报告的建议在 GDPR 合规负责人或 DPO 的监督下就相关问题进行整改，同时追究有关人员的相应责任。

1. 针对特定业务模块的监督和审计

建议企业的内部审计部门以业务模块为划分，定期开展对 GDPR 合规制度落实和执行情况的审计。企业在进行针对业务模块的 GDPR 合规情况的审计之前，可由审计人员与企业内部 GDPR 合规负责人及企业所设 DPO（如有）进行咨询，共同确定出审计所要覆盖的范围并制定详细的审计方案，明确审计的目的、范围、程序、方法、技术、人员、期限等内容。在审计结束之后，可由审计人员就各个业务部门针对 GDPR 合规制度执行情况的充分性和有效性出具书面审计报告。

企业 GDPR 业务模块审计报告中需载明：（1）该业务部门 GDPR 合规制度的整体执行概况；（2）审计依据；（3）审计中所发现的主要风险和执行问题；（4）针对审计中发现的问题所提出的审计建议；等。

2. 定期全面审计

企业的内部审计部门每年应当就 GDPR 的合规制度进行全面审计。不同于定期的 GDPR 业务模块合规审计，企业的 GDPR 年度全面审计是以定期的 GDPR 业务模块合规审计的结果为基础，对定期的 GDPR 业务模块合规审计后的整改情况进行梳理，并结合定期的 GDPR 业务模块合规审计中所发生的问题，从整体上对合规制度和业务流程进行改进和优化，并对企业法律文本进行审查，保证企业的法律文本同步作出调整和更新。

1）对合规制度和业务流程的改进和优化

在进行年度全面审计时，建议企业审查企业在整体合规制度完善程度以及业务流程设置上的合理性，并结合定期的 GDPR 业务模块合规审计过程中所发现的不同业务环节和业务流程中的 GDPR 合规问题，在审计报告中进行披露，并就合规制度的完善以及业务流程的改进和优化提出审计建议，以最大限度地避免类似合规问题的重复出现。

2）对内部文本和第三方文本的进一步调整和更新

建议企业结合其在定期的 GDPR 业务模块合规审计中所发现的问题，以及经审计后所采取的整改措施，在年度全面审计中对企业内部及外部文本进行逐个排查，审查企业内外部文本的合规性。对于审计中发现的可能存在问题的法律文本，审计人员可就该文本及其对应的问题在审计报告进行披露，并针对所存在的问题和风险提出调整和更新的建议。

3. 向监管机构(DPA)的咨询

企业的相关业务部门和审计部门对于企业 GDPR 合规制度执行及对审计过程中所涉及的事项存在疑问的，可以向企业 GDPR 合规负责人或企业所设的 DPO（如有）进行咨询。经 GDPR 合规的负责人或 DPO 认为可能存在风险但无法进行确定性判断的，可以暂时停止可能存在风险的相关处理活动，经 GDPR 合规负责人或 DPO 与管理人员合议后，由 GDPR 合规负责人或 DPO 向主管的监管机构就相关事项的风险性向监管机构进行咨询，以确定是否可以继续相关处理活动或就相关事项采取整改措施。

4. 投诉与举报

针对就企业 GDPR 合规的相关问题所作出的投诉和举报，企业需予以充分重视。建议企业建立相应的投诉与举报的反应机制，并以被投诉或被举报事项为轴心，对企业业务中存在的合规风险进行排查，降低举报或投诉可能给企业带来的损害。具体而言，建议企业建立如下机制：

一方面，建议企业建立与投诉人或举报人的沟通机制，确保企业在收到投诉与举报后，企业的突发事件处理人员能够及时与投诉人或举报人开展沟通，了解投诉与举报的原因、所依据的理由或证据，初步判断所举报或投诉事项的真实性。

另一方面，建议企业建立投诉或举报的事件应急处理机制。例如企业可以规定：收到投诉与举报的人员和部门应及时向 GDPR 的合规负责人员进行汇报；GDPR 的合规负责人员经对举报的真实性进行初步判断后决定是否展开调查；经 GDPR 合规负责人员决定需要开展调查的，GDPR 合规负责人员可以向管理层进行报告，同时组建内部调查工作小组，由 GDPR 合规负责人员牵头，对于所举报的事项开展内部调查。

此外，建议企业以制度的形式明确相关业务部门对调查小组工作开展的配合义务，并规定调查小组开展工作的具体方式。例如，企业可以规定：

（1）调查小组开展内部调查时，可以根据投诉举报中所提供的线索和证据确定被举报行为或事项所处的业务流程和所涉的业务范围，从而锁定风险范围开展核查。除此之外，调查小组还可以以投诉或被举报事项中所涉及的问题为切入点，对于企业中其他可能涉及到该问题的业务进行排除，最大限度地降低潜在风险。

（2）调查小组开展内部调查时所采取的方式，可以包括人员访谈、文件审查等。调查小组在调查取得阶段性进展或发现重大风险时，需及时向董事会进行报告。调查结束后，调查小组可就调查情况形成调查报告，报告中需写明调查中所发现的主要问题并提出对应的整改措施。调查报告需呈交董事会下设的合规专门委员会或主管数据合规的相关负责人。专门委员会或主管数据合规的相关负责人对报告作出批准意见后，相关部门应当按照调查报告所提出的要求进行整改。

5. 应对监管机构的调查

监管机构对企业的 GDPR 合规情况开展调查时，建议企业安排 GDPR 合规负责人员或 DPO 作为负责人员与监管机构进行对接，并对调查机构开展调查活动的进行记录，了解监管机构的关注重点，配合执法机构开展调查活动，积极开展企业内部的自查工作。对于监管机构经过合法调查所发现的 GDPR 合规问题，企业最好应按照监管机构的要求及时采取措施进行整改。

三、GDPR 疑难点及合规建议

（一）GDPR 的域外适用

Q：中国境内的欧盟个人数据管不管？

A：GDPR 不适用于欧盟国家公民在欧盟范围外接受服务时提供自己的个人信息的情况，只要这些信息的采集和处理过程均是在欧盟境外完成。在下面的案例中，服务提供者并不需要将 GDPR 作为其处理欧盟国家护照持有者的个人信息时的准则，而只需要遵守服务提供地的法律。例如，一个推荐北京的餐厅的中文版手机 APP，可以让身处北京的法国人通过其预定餐厅或者获得优惠，无需遵守 GDPR 的要求收集、使用或处理该法国人的数据。

值得注意的是，如果存储于中国境内的欧盟个人数据是企业通过提供面向欧盟的服务而在线收集而来，则 GDPR 对其适用。例如，该 App 有法语版本，并在法国宣传其可为法国游客在中国旅行提供服务，则该法国用户的数据受 GDPR 管辖。

（二）个人数据的范围

Q：GDPR 中的个人数据指的是哪些数据？

A：个人数据是指任何指向一个已识别或可识别的自然人的信息。该可识别的自然人能够被直接或间接地识别，尤其是通过参照诸如姓名、身份证号码、定位数据、在线活动识别符，或者是通过参照针对该自然人一个或多个如物理、生理、遗传、心理、经济、文化或社会身份的要素。实践中，个人数据还包括通过任意一种方式被分配或可被分配给某人的所有数据。例如，电话号码、个人的信用卡或人员编号、账户数据、号牌、外貌和客户号或地址，均属于个人数据。

经过假名化处理的数据可以使识别个人更加困难，从而降低隐私风险，但其仍属于个人数据。如果个人数据可以被真正地匿名化处理，那么经过匿名处理的数据不受 GDPR 规制。

在 GDPR 下，数据保护并不适用于有关诸如公司、基金会以及机构等法律实体的信息。

除了一般的个人数据以外，还有特殊类别的个人数据（也被称为敏感个人数据）。这些数据包括基因、生物识别和健康数据，以及可被归于某一个人的种族

和族裔血统、政治意见、宗教或意识形态信念或某一社群组织的成员关系的个人数据。

Q：在线活动识别符（Online Identifier）具体包括什么？

A：GDPR 在个人信息的定义中特别地包括了“在线活动识别符”这一概念，其包括与个人使用的设备、应用、工具及互联网协议等相关的信息。GDPR 序言第 30 条中对在线活动识别符进行了一个非穷尽式的列举：

- 互联网协议地址（IP 地址）
- Cookie 识别符
- 射频识别（RFID）标签等其他识别符

其他可能属于个人数据的在线活动识别符包括：

- MAC 地址
- 广告 ID
- 像素标签
- 设备指纹

对于上述在线活动识别符所留下的痕迹，当与服务器所接收的特殊识别符或其他信息相结合后，可以用来对个人进行画像并识别个人。

在评估个人是否可识别时，企业必须考虑在线活动识别符自身或者与其他信息结合后是否会被用来将个人与其他人区分，区分的方法可能是对用户进行画像以识别个人。

（三）如何理解数据处理的 6 个合法事由？

Q：什么是履行合同之必要？

A：GDPR 第 6 条规定了处理数据的 6 种合法事由，其中包括数据主体为履行合同之必要，或者在合同订立前应数据主体的要求而采取某些与订立合同相关的行动而处理数据。

通常在以下两种情况下，可以将履行合同之必要作为合法事由：

- 企业与个人之间存在着一份合同，为了履行该合同项下的义务，企业需要处理某些数据主体的个人数据。

- 企业与个人之间尚未达成一份合同，但数据主体要求企业采取某些行为作为第一步（例如，提供一个报价），为了完成数据主体所要求的行为，企业需要处理其个人数据。

“必要”并不意味着数据处理行为对于达成合同或进行相关前置步骤的目的来说是必须的，但数据处理行为必须是为实现上述目的的且恰当的方式。如果存在其他合理且侵扰性较小的方式来履行企业的合同义务或完成数据主体的要求，则该合法事由不适用。

另外，如果该合同是与 18 岁以下的儿童签订，企业还需要考虑他们是否具备签订合同的行为能力。如果企业对其行为能力存有疑虑，企业可以考虑其他替代性的合法事由，例如合法利益，该事由可帮助企业证明该儿童的权益已被恰当地考虑和保护。

企业应记录此类决策，即处理数据的行为对于合同来说是必要的，记录中应当包括企业隐私通知中所披露的处理目的及合法事由。

Q：什么场景下可以使用数据控制者的正当利益作为数据处理合法事由？

A：正当利益是 GDPR 下的另一种合法事由。GDPR 第 6 条规定，如果个人数据的处理对于控制者或第三方所追求的正当利益是必要的，企业可以处理个人信息，除非要求对个人数据进行保护的数据主体利益或基本权利及自由超过了上述正当利益，尤其是数据主体为儿童时。正当利益事由可以被拆解成以下三个层面加以理解：

- 目的测试：企业所追求的是否是正当利益？
- 必要性测试：对于该目的而言，个人数据处理是否必要？
- 权衡测试：个人权益的保护是否胜过企业追求的正当利益？

GDPR 尤其将“对于客户或雇员数据的使用”、“推广营销”、“欺诈防护”、“集团内部转移”或“IT 安全”列为潜在的正当利益，但这并非穷尽式的列举。GDPR 还规定，向政府机关披露与可能的刑事犯罪行为或安全威胁有关的信息，对企业来说也构成正当利益。

当企业可以合理期待的方式使用数据，并且这种方式在对数据主体隐私方面的影响最小，那么正当利益可能是最为适当的合法事由。在对个人存在一定影响的情况下，如果能证明处理个人数据可以带来更具说服力的益处，并且能够证明

产生的影响是合理的，则正当利益仍可适用。企业可以考虑根据正当利益处理儿童的数据，但在这种情况下应当尽到更多的注意义务确保儿童权益得到保护。

（四）如何理解数据主体的几个权利？

Q：如何理解自动化决策与用户画像？

A：针对个人的自动化决策是指通过自动化手段做出的决定，没有任何人工参与。例如：

- 决定是否授予贷款的在线决策；以及
- 使用了预先编程算法及标准的招聘能力测试。

针对个人的自动化决策并不一定涉及到用户画像，虽然实际上经常两者并用。根据 GDPR，用户画像是指“任何形式的个人数据自动处理，只要这种处理包括了使用个人数据评估有关自然人的某些个人方面，尤其是分析或预测有关自然人在工作中的表现、经济状况、健康、个人偏好、兴趣、可靠性、行为、位置定位或移动”。针对个人的自动化决策以及用户画像有助于实现更为快捷、协调的决策，但如果使用不当，则会对个人造成严重风险。GDPR 的相关条款旨在规制这些风险。

GDPR 限制企业进行对数据主体产生法律影响或具有类似重要影响的完全自动化决策，包括基于用户画像的自动化决策。“完全自动化”指的是决策过程中没有任何人工参与。“法律影响”指的是对某类个人的法律权利产生的不利影响。“类似重要影响”更难被定义，但包括了例如自动拒绝在线信贷申请、数字化招聘等没有人工干预的实践做法。

在以下三种情况下，企业可以进行自动化决策：

- 对于组织与个人之间订立合同或履行合同来说是必要的；
- 由法律授权（例如，反欺诈或反税收侵蚀）；或
- 基于数据主体的明示同意。

如果使用特殊类别的个人数据，企业仅可以在以下两种情况下进行自动化决策：

- 企业获得了数据主体的明示同意；或
- 数据处理对于重大公共利益而是必要的。

从企业合规角度考虑，对于自动化决策，企业应做到：

- 提供有关决策过程涉及的逻辑、对数据主体的重要性和预期后果有关的信息；
- 使用适当的数学或统计程序；
- 确保数据主体可以获得人工干预、表达其观点，能够获得该决策的解释并对其质疑；
- 采取适当的技术和组织措施，以便企业可以纠正不准确之处并将错误风险降至最低；
- 采用与数据主体权益风险成比例的方式保护个人数据，并防止歧视性影响。

目前在实践中，企业也会对用户就自动化决策与用户画像的情况进行披露，例如：

1. Google 您可以前往广告设置部分控制我们可以利用哪些信息来向您展示广告。

2. Apple 自动决策制定(包括受众特征分析)的存在：Apple 不会在算法的使用或会给你带来重大影响的受众特征分析方面做出决策。

（五）数据控制者和数据处理者的区别

Q：数据控制者和数据处理者的义务有何区别？

A：在 GDPR 下，数据控制者和数据控制者所承担的实体义务大致有如下区别：

数据控制者	数据处理者
• 确保数据处理的合法基础（第 6 条及第 9 条，如果涉及敏感个人数据） • 符合基本的处理原则：有限目的、数据最小化/存储限制、完整性和保密（第 5 条） • 遵守并协助数据主体权利，例如，访问、更正、删除、限制、反对及可携权（第 15、16、17、18、20 及 21	• 确保未获得处理者授权的主体不得处理个人数据，除非根据数据处理者的指示（第 29 条） • 保存数据处理活动的记录（第 30 条） • 实施与数据处理风险相适应的安全措施（第 32 条） • “没有不当拖延”地通知数据控

条） • 保存数据处理活动的记录（第 30 条） • 数据泄露强制通知（72 小时之内向监管机关通知）以及通信要求 • 确保数据处理者为符合 GDPR 要求而提供“足够的保障”，并确保所有处理活动都根据规定了特定强制性内容的书面协议而进行（第 28 条） • 实施与数据处理风险相适应的安全措施（第 24 及 32 条），并确保“从设计着手保护隐私”（第 25 条） • 进行数据安全影响评估，并就高风险处理咨询监管机关（第 35 条） • 没有合法基础的情况下，不得将个人数据转移至欧洲经济区之外（第 49 条）	制者数据泄露事件（第 33 条） • 确保所有处理活动都根据规定了特定强制性内容的书面协议而进行（第 28 条） • 没有合法基础的情况下，不得将个人数据转移至欧洲经济区之外（第 49 条）

（六）数据控制者和数据处理者的责任

Q:如何设定数据保护官？

A：GDPR 第 37 条规定了数据控制者和数据处理者应当任命 DPO 的情形，包括：（1）公权力部门或机构进行数据处理活动的；（2）数据处理的核心活动涉及对数据主体进行经常性大规模系统化监测的；（3）大规模处理特殊类别个人数据或与刑事违法行为相关的个人数据的。除上述情形之外，GDPR 并未要求企业在其他情形下也进行 DPO 的设置。

GDPR 并未对“大规模”的概念进行定义。第 29 条工作组发布的指引认为，“无论是处理的数据量还是涉及到的数据主体数量方面，均无法给出准确的数字。”指南建议，应当考虑下列因素：

- 有关数据主体的数量——作为一个具体数量或相关人数的一部分
- 据量和/或各类不同数据项的范围
- 持续时间或持久性；以及
- 个人数据处理活动的地理范围

（1）DPO 的选任

根据 GDPR 的要求，企业对于 DPO 的选任应当结合企业可能涉及到的数据处理活动以及数据保护要求，从职业能力、数据保护法律方面的专业知识、实践经验和能力要求等方面进行考量，确保其有能力完成 GDPR 项下所规定的各项职责。

从 GDPR 的规定来看，DPO 既可以是企业的雇员，也可以是企业之外通过合同的形式向企业提供服务的专业人员。鉴于上述规定的灵活性，建议企业根据实际业务的情况进行选择。但是一般而言，如果企业涉及 GDPR 规制的业务活动类型较多、范围较大，则通过合同形式任命外部人员担任 DPO 可能存在较大风险，可行性较低。在该种情形下，企业任命其已具备相应知识和能力的雇员作为 DPO 更为稳妥可行。

企业确定所要任命的 DPO 之后，应当确保监管机构能够及时与 DPO 取得联系。因此，建议企业以一定的可为公众所知的形式公布 DPO 的联系方式，并向监管机构进行报告。此外，如果作为数据控制者或处理者的企业在欧盟境内设有实体，则建议企业根据自身实际情况的需要，考虑是否将 DPO 设置在欧盟境内，便于其与监管机构之间顺畅有效的沟通。

（2）DPO 的职责范围

企业设置的 DPO 并非仅仅向企业提供服务，而是具有服务企业和对接监管机构的双重职能。根据 GDPR 的规定，DPO 至少应当承担以下职责：

- 向企业或其他数据处理人员进行通知和提出建议；
- 监控企业对 GDPR、成员国立法、企业内部规定等的遵守情况；
- 根据 GDPR 的有关规定对数据保护影响评估和监控提出建议；
- 与监管机构进行合作；
- 作为监管机构监管数据处理活动的联系点并开展协调活动

针对 GDPR 所规定的上述职责，建议企业以制度的形式赋予 DPO 履行职责所必需的权力、资源和人员，并定期开展或支持 DPO 参加专门针对 DPO 的相关数据培训，以保障 DPO 具体职责的履行。

Q:数据处理者如何履行问责义务（accountability）？

A：问责义务包含两个关键要素。首先，问责制原则明确规定，企业有责任遵守 GDPR。其次，企业必须能够证明自身的合规性。

负有遵守 GDPR 的责任意味着在有关数据保护的方式上，企业需要做到积极主动、组织有序。同时，对企业的合规性予以证明也意味着企业必须能够证明为了合规所采取的步骤。

为了做到这一点，企业可以进行以下几方面工作：

- 实施数据保护内部政策——GDPR 明确指出，在合适的情况下，实施数据保护的内部政策是企业可以采取的用以确保并证明合规性的措施之一。企业内部制度的具体内容及其详细程度取决于企业如何处理个人数据。

- 采用“从设计角度并默认保护数据”方法 ——“从设计角度并默认保护数据”是尽责的一个组成部分。其含义是将数据保护嵌入到企业执行的所有操作中，贯穿所有的个人数据处理操作。GDPR 建议采取一些适当的措施，例如最小化企业收集的数据，应用假名化处理技术以及改进安全功能。

- 书面合同——每当数据控制者使用数据处理者来代表他们处理个人数据时，需要签订一份书面合同，规定各方的责任和义务。合同必须至少包括某些特定条款，例如要求数据处理者采取适当措施以确保处理的安全性，并要求其有协助数据控制者的义务，允许个人行使其在 GDPR 下的权利。

- 留存记录——根据 GDPR 第 30 条的要求，大多数企业组织必须保留其个人数据处理活动的记录，包括处理目的、数据共享和留存等内容。

- 安全措施——GDPR 重申了采取技术和组织方面的措施以在安全方面遵守 GDPR 的要求。除此之外，这可能包括信息安全内部制度、访问控制、安全监控和恢复计划。

- 记录和报告个人数据泄露事件——企业必须向相关监管机构报告某些类型的个人数据泄露，在某些情况下，还要向受影响的个人报告。此外，GDPR 规定，无论企业是否需要报告，企业必须记录下任何的个人数据泄露事件。

• 开展数据保护影响评估——数据保护影响评估是一项必要的落实问责制的工具，也是通过采用设计的方式将数据保护导入企业行为中的关键部分。 它可以帮助企业识别和最小化企业承担的任何新项目中的数据保护风险。

（七）个人数据出境的合法事由

Q：中国企业可适用的数据出境方式是什么？

A：根据 GDPR 的规定，将欧盟境内个人数据转移至其他司法管辖区时应区分安全和非安全两类第三方司法管辖区。安全的第三方司法管辖区是指欧盟委员会已经确认的具有充分数据保护水平的司法管辖区，其国内法提供了与欧盟法相匹配的数据保护程度。目前，通过上述充分性认定的司法管辖区包括：安道尔、阿根廷、加拿大（仅包括商业组织）、法罗群岛、根西岛、以色列、马恩岛、瑞士、乌拉圭和美国（如果数据接受者适用隐私盾）。对上述司法管辖区的数据转移被明确允许。2019 年 1 月，欧盟与日本之间达成个人数据跨境传输充分性框架，可以在欧盟与日本之间实现个人数据的双边自由传输。

对于其他司法管辖区，应确保数据接收方能够提供充分的数据保护。相关机制包括签署标准合同条款、集团公司内部采纳“约束性公司规则”、遵守欧盟委员会公布的通常适用的行为规则或通过数据处理程序认证。

对于中国企业，常见的数据出境方式是由欧盟境内的主体与境外数据接收主体签订标准合同条款，并根据此条款进行数据跨境转移。

（八）主监管机构的理解

Q：如何确定主监管机构？

A：GDPR 在欧盟数据保护法中引入了“主营业地”（Main Establishment）原则，其主要影响是当企业在欧盟有多个营业地时，其将决定企业的监管机构。该监管机构将会是企业在 GDPR 的执法以及相关合规问题上的首要联系方，例如 (i)第 34 条下的违反数据保护义务通知；(ii)第 35 条下的隐私影响评估；(iii)第 36 条下的隐私影响评估后期咨询义务，这是 GDPR 所引入的一站式监管机制。

需要注意的是，一家公司可能会有多个主营业地，这取决于所涉及到的数据处理操作。例如，人力资源数据处理的主营业地可能会不同于客户数据处理的主营业地。因此，主营业地的确定应当根据不同类型的个人数据处理操作分别进行。

GDPR 规定，某一组织的主营业地是有权就该组织处理欧盟个人信息进行决策并对此负有整体责任的欧盟实体。主营业地通常是该组织进行有效、实际的组织管理活动的地点。帮助企业确定主营业地的要件包括：

- 谁可以进行处理个人信息目的和方法的最终决策；
- 谁决定涉及个人信息处理的业务活动；
- 谁有权将决策付诸实施；以及
- 负有总体管理责任的管理者所在地。

可能存在很难指定出主营业地的情况，因为没有单个实体具有所要求的控制者能力，且决策权并非中心化或者可能仅由欧盟外的实体拥有。在这种情况下，企业可以采取一些方法，使得整体情况有利于认定出一个至少具有一定能力来执行个人数据处理决策的特定主营业实体。但请注意，监管机关可能会对所宣称的主营业实体地位提出质疑，并将另一个机构考虑为主营业实体。

主营业实体设立地的欧盟成员国的监管机关将有资格成为主监管机关。主监管机关将对公司进行 GDPR 的相关执法。如果个人数据处理操作仅与另一成员国的某一企业有关，或仅对另一成员国的个人有影响，则其他成员国的监管机关仍有执法权，除非主监管机关决定处理该问题。同样，如果有关违法行为违反成员国本国法律，当地的监管机关也有执法权。

Q：欧洲数据保护委员会和各国监管机构如何配合执法

A：根据 GDPR 第 51 条的规定，为了保护自然人在数据处理过程中的基本权利和自由，并促进个人数据在欧盟中的自由流动，每个成员国应规定一个或多个独立的公共机构负责监督本法规的实施。每个监管机构应在整个欧盟内为本法规的一致适用做出贡献。

欧洲数据保护委员会是一个独立的欧盟机构，致力于在整个欧盟范围内数据保护规则的统一适用，并促进欧盟数据保护机构之间的合作。EDPB 还被授权通过作出有约束力的决定来对跨境个人数据处理活动的争议作出裁决，从而确保欧盟规则的统一应用，以避免同一案件在不同司法管辖区内可能被不同方式处理。

对于 EDPB 与各成员国监管机关的关系，EDPB 在监督机构起草决定的过程中扮演提供意见的角色。除此之外，EDPB 还需要在三种情况下发布具有约束力的决定。这些案件主要涉及监管机构之间的争议解决：

- 当有关监管机构对主监督机构的决定提出异议，或主监督机构驳回异议时（一站式机制）；
- 就哪一监管机构是主监管机构的问题出现了分歧性看法时；
- 当监管机构没有征询 EDPB 的意见（一致性机制所要求的意见）或不遵循 EDPB 的意见时。

四、GDPR 与我国法律的比较及冲突应对

（一）中国个人信息保护法律规则与 GDPR 的比较

企业在进行 GDPR 合规时都会面临这样的一个问题，即 GDPR 对企业合规的要求与中国个人信息保护法律规则有什么区别？如何在已有合规体系的基础上满足 GDPR 的合规要求？而与此同时，又有不少在中国经营的跨国企业则先一步完成 GDPR 合规，需要完成国内法的对接。本部分将从对比 GDPR 和国内个人信息保护的法律、法规入手，为希望开拓欧盟市场的中国企业与在中国经营的跨国公司提供两个不同法域的合规对接。

近两年来，中国在个人信息保护方面立法频繁：在行政法领域，2017 年开始施行的《网络安全法》，延续了 2012 年《全国人民代表大会常务委员会关于加强网络信息保护的决定》、2013 年《电信和互联网用户个人信息保护规定》、2013 年《消费者权益保护法》等关于个人信息保护的思路，并将对个人信息保护的作为网络安全的重要组成部分，明确了“个人信息”的概念，规定了个人信息保护原则和网络运营者应承当的法律义务；在民法领域，2017 年公布的《民法总则》，首次对隐私权和个人信息采取“二元论”保护模式 ；在刑法领域，2015 年的《刑法修正案九》将“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”整合为“侵犯公民个人信息罪”，放宽了侵犯公民个人信息罪的主体范围；2017 年生效的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称“两高司法解释”）在《网络安全法》的基础上，进一步扩大了个人信息的定义范围，将反映特定自然人活动情况的各种信息，例如行踪轨迹信息等均纳入到个人信息保护范畴，同时明确了此罪的认定标准和量刑标准。在国家安全标准领域，2017 年底颁布、2018 年 5 月正式施行的国家标准 GB/T 35273-2017《信息安全技术 个人信息安全规范》（以下称“《个人信息安全规范》”）在《网络安全法》基本原则的基础上，借鉴了大量 GDPR 的规则思路，有利于企业个人信息保护合规与国际规则（如 GDPR）的接轨，并且是我国首部系统的个人信息保护规范，也是中国互联网企业个人信息保护的重要参考指南，上述规范（统称为中国个人信息保护规则）构成了在中国境内经营的企业的个人信息保护规则。施行近一年后，该标准进行了修订，并于 2019 年 1 月 30 就修订稿草案向社会公开征求意见。

1、《个人信息安全规范》与 GDPR 共通点

中国个人信息保护规则与 GDPR 共通之处在于都引入了国际通行的个人信息定义标准、原则和权利框架及个人信息风险控制理念等先进规则。总体看，中国个人信息保护规则通过一系列法律及标准规则的完善，特别通过《个人信息安全规范》与 GDPR 的对接，其基本的个人信息保护的原则和大的框架是一致的，主要表现在：

（1）共通的个人信息界定标准。中国个人信息保护规则与 GDPR 均采用了“识别”或“关联”的标准。即只要“已被识别”与个人相关或能够“反映特定自然人活动情况”的信息都属于个人信息。作为对大数据时代个人信息处理的回应，均将网络识别信息和网络行为信息纳入个人信息的范围。

规则点相同共通点	中国个人信息保护规范	GDPR
个人信息的内涵	是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。（《网安法》第 76 条）	指一个被识别或可识别的自然人(“数据主体”)的任何信息（第 4 条）
	以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。（《个人信息安全规范》）	

（2）趋同的个人信息保护原则和权利保护框架。中国个人信息保护规则与 GDPR 均依据国际通行的个人信息保护原则，包括透明度、目的限定、最小够用、权责一致等。在权利设置上包括查询、更正、删除等个人信息权利设置。

规则点相同共通点	中国个人信息保护规范	GDPR
个人信息保护原则	合法、正当、必要的原则(《网安法》第 41 条)	合法、公平、透明原则 、目的限制、最小化原则 、准确性原则、存储限制(必要最短)、完整、保密原则、权责一致原则（第 5 条）
	权责一致原则、目的明确原则、选择同意原则、最少够用原则、公开透明原则、确保安全原则、主体参与原则（《个人信息安全规范》）	
个人信息主体权利	知情权、修改权、删除权 《网安法》	知情权、信息获取权、修改权、被遗忘权（第 13.14 条）
	知情权、信息获取权、修改权、删除权	

	（《个人信息安全规范》）	

（3）同意的例外与对企业合法利益的考量。GDPR 不是一味的强调个人信息主体的自决权，根据 GDPR 第六条的规定，当其他权利和合法事由高于个人信息主体自决权时，个人的权利须让渡于其他权利与合法事由。我国《个人信息安全规范》对此进行了借鉴，规定了收集、使用个人信息无需征得个人信息主体的授权同意的例外，这也是《个人信息安全规范》在法律规定基础上的最大创新。

规则点相同共通点	中国个人信息保护规范	GDPR
同意的例外	以下情形中，个人信息控制者收集、使用个人信息无需征得个人信息主体的授权同意： a) 与国家安全、国防安全直接相关的； b) 与公共安全、公共卫生、重大公共利益直接相关的； c) 与犯罪侦查、起诉、审判和判决执行等直接相关的； d) 出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人同意的； e) 所收集的个人信息是个人信息主体自行向社会公众公开的； f) 从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道； g) 根据个人信息主体要求签订和履行合同所必需的； h) 用于维护所提供的产品或服务的安全稳定运行所必需的，例如发现、处置产品或服务的故障； i) 个人信息控制者为新闻单位且其在开展合法的新闻报道所必需的； j) 个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的； k) 法律法规规定的其他情形。	**GDPR 的表述是数据处理的合法事由，**除基于同意：数据控制者的合法利益所必须，外，还包括： 为履行数据主体作为一方的合同所必须；为履行数据控制者的法律义务所必须；为保护数据主体或另一自然人的重大利益所必须；为实现公共利益所必须；其中后 3 必须在欧盟法或成员国法中明确规定（GDPR 第 6 条）

（4）引入以风险控制为中心的个人信息保护理念。中国个人信息保护规则与 GDPR 均会平衡个人信息自主权与社会公共利益、企业及其他主体的合法权益。均规定对于个人信息主体的权利请求，要综合考虑可能对个人信息主体合法

权益带来的风险和损害、技术可行性、以及实现请求的成本的成比例性等因素后，确定如何实现个人信息主体的权利。此外，中国个人信息保护规则与 GDPR 均引入了 DPO、个人信息影响评估、问责制、去标识化（假名化）、加密等风险控制的个人信息保护规则和手段。

规则点相同共通点	中国个人信息保护规范	GDPR
组织人员要求	**人员要求：**应任命个人信息保护负责人和个人信息保护工作机构。个人信息保护负责人和个人信息保护工作机构应履行以下职责：1)全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任；2)制定、签发、实施、定期更新隐私政策和相关规程；3)应建立、维护和更新组织所持有的个人信息清单（包括个人信息的类型、数量、来源、接收方等）和授权访问策略；4)开展个人信息安全影响评估；5)组织开展个人信息安全培训；6)进行安全审计。（《个人信息安全规范》）	**数据保护官：**公共组织（法院除外）、核心业务涉及对用户进行经常性的大规模的系统性监控的企业、核心业务涉及处理个人敏感数据或者与刑事犯罪有关的个人数据的企业，应当任命一个数据保护官。多个相关企业可以委任一个数据保护官。 数据保护官的职责包括：通知和建议企业履行其在 GDPR 之下的义务；监测企业履行其义务；与监管部门合作。（第 37 条）
安全技术措施	网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。（《网安法》第 42 条）	对个人数据的匿名化和假名化； 确保提供持久的机密性、完整性、可用性和系统可恢复性的能力； 在物理或者技术事故下及时回复数据可用性、可访问性的能力 建立定期测试、评估、评价技术和管理措施是否有效的体系
	去标识化处理 收集个人信息后，宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信息处理中不重新识别个人。 个人敏感信息的存储 1.存储个人敏感信息时，应采用加密等安全措施； 2.存储个人生物识别信息时，应采用技术措施处理后再进行存储，例如仅存储个人生物识别信息的摘要。（《个人信息安全规范》）	
记录义务	处理活动的记录 •散见于《网安法》、个人信息和重要数据跨境安全评估办法及指南、网络安全检查指南等•《安全规范（报批稿）》如 规定了准确记录个人信息委托处理、共享、转让及披露情况的义务 e) 个人信息控	数据控制者必须全面记载其数据处理活动，做到一举一动都有据可查。包括数据处理的目的、数据的类型、数据接收者的类别以及转移至第三国的数据接收者、数据

	制者应准确记录和保存委托处理个人信息的情况。准确记录和保存个人信息的共享、转让的情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等；准确记录和保存个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等；发生个人信息安全事件后，个人信息控制者应根据应急响应预案进行以下处置：1) 记录事件内容， •《安全规范》第 10.5 条 安全审计 应建立自动化审计系统，监测记录个人信息处理活动；	保存的时间、采取的安全保障措施等等，保留有与数据处理者的合同附件。 不适用情形： 员工规模在 250 人以下的企业或组织，除非处理行为可能给数据主体的权利和自由造成风险； 偶然发生的处理活动，除非处理活动包括特殊种类的数据，或者包括刑事犯罪定罪和罪行相关的个人数据。（第 30 条）
个人信息影响评估	•建立个人信息安全影响评估制度，定期（至少每年一次）开展个人信息安全影响评估； •个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响，内容包括但不限于： 1.个人信息收集环节是否遵循目的明确、选择同意、最少够用等原则； 2.个人信息处理是否可能对个人信息主体合法权益造成不利影响； 3.个人信息安全措施的有效性； 4.匿名化或去标识化处理后的数据集重新识别出个人信息主体的风险； 5.共享、转让、公开披露个人信息对个人信息主体合法权益可能产生的不利影响； 6.如发生安全事件，对个人信息主体合法权益可能产生的不利影响。（《个人信息安全规范》）	当处理个人数据采用新技术，可能影响自然人的权利和自由时，企业在开展个人数据处理之前，应当先行对新技术可能给个人数据保护带来的影响进行评估。 在下列情形中，尤其应当开展影响评估： 涉及基于自动化处理对用户进行画像等决策； 涉及处理个人敏感数据； 涉及处理与刑事犯罪有关的个人数据； 涉及对公共区域进行大规模的系统性监控。 当数据保护影响评估显示，如果不采取措施减少相关风险，数据处理行为就会产生较高风险，企业就应当在开展数据处理之前，先行咨询监管部门。（第 35 条）
数据泄露通知	在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。(《网安法》第 42 条)	当发生个人数据泄露事件时，企业必须于知悉该事件后的 72 小时内通知监管部门，除非该事件不大可能给自然人的权利和自由带来风

	规定了详细的需要告知的事项及告知方式：对个人信息控制者的要求包括： a) 应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息； b) 告知内容应包括但不限于： 1) 安全事件的内容和影响； 2) 已采取或将要采取的处置措施； 3) 个人信息主体自主防范和降低风险的建议； 4) 针对个人信息主体提供的补救措施； 5) 个人信息保护负责人和个人信息保护工作机构的联系方式。（《个人信息安全规范》）	险；倘若在 72 小时内未能通知监管部门，企业应当于随后通知之时附带说明延迟的理由。通知的内容包括个人数据泄露事件的性质，涉及的用户的类型和数量，泄露的个人数据的类型和数量，个人数据泄露事件可能造成的后果，将会采取的措施。 通知受到实质性影响的用户：当个人数据泄露事件可能影响自然人的权利和自由时，企业应当及时通知相关用户，通知的语言应当清楚、直白。如果数据控制者采取了适当的保护措施，特别是采取的措施能够使得数据难以被一般人所理解，比如加密，或者其后续采取的措施能够使得威胁不会成为实际的结果则无需通知。（第 33 条）

（二）中国个人信息保护规则与 GDPR 的区别

中国个人信息保护规则与 GDPR 的区别主要体现在对于敏感个人信息的认定、同意的标准及用户个人信息自决权的形式范围等。

1、个人敏感信息范围和处理限制的区别

中国的个人信息保护规则基于个人信息泄漏后对个人的人身和财产安全的受损程度的不同，将严重一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息定义为个人敏感信息。而 GDPR 规定的个人敏感信息主要是基于对个人种族、性别等可能会导致歧视性待遇的隐私的保护。因此中国的个人敏感信息的范围要广于 GDPR 的规定。因此也决定了 GDPR 规定敏感个人信息原则上不允许处理，而中国个人信息保护规范要求在征得明示同意后即可处理。

规则点差异	中国个人信息保护规范	GDPR
个人敏感信息	一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。（范围广，不禁止处理，但须满足更高的要求） 个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。范围比 GDPR 大很多。 **收集个人敏感信息时须明示同意** （《个人信息安全规范》）	特殊类别（敏感）个人数据:揭示种族或民族出身，政治观点、宗教或哲学信仰以及工会成员的个人数据，以及唯一识别自然人为目的的基因数据、生物特征数据、自然人的健康、性生活或性取向数据等，GDPR 从收集、使用等角度作出了特殊规定。(与个人的身份和隐私相关的个人数据），原则上禁止处理。**（第 9 条）**

2、“同意”的区别

《个人信息安全规范》与 GDPR 的主要区别基于《网络安全法》等现有法律原则性规定与 GDPR 的不同。GDPR 的个人信息处理可以基于履行合同之必要、个人信息主体同意、履行法定义务、保护重要利益、公共利益以及控制者的优先利益等六种合法事由。因此用户“同意”并不是唯一的数据收集和使用的一种合法事由。所以 GDPR 只有一种同意的标准。根据 GDPR 第 7 条规定，“同意”必须是具体的、清晰的，是用户在充分知情的前提下自由做出的。如果数据控制者希望获得的同意的事项区别于此前已取得同意的事项范围，则需要向用户做出单独明确的说明；如果将同意数据处理作为签订合同的前提条件，而这种数据处理事实上超出了提供服务所必需的范围，将违反有关“同意应当是自由做出”的规定。因此 GDPR 的同意可理解为中国的“明示同意+可撤销同意”。

但《网络安全法》等现有的个人信息保护基本框架可概括为“用户知情同意+安全保障义务”。而《个人信息安全规范》不能超出网安法的基本框架设定标准。如何在既定的法律框架下实现基于风险等级不同的个人信息自主权实现模式？《个人信息安全规范》一是基于个人信息自主权与公共利益及其他合法权益的平衡，规定了 11 项收集、使用个人信息无需经个人信息主体同意的情形，二是一方面基于泄露后可能给个人信息主体造成的危害程度将个人信息区分为敏感个人信息和一般的个人信息，另一方面是基于个人收集和使用的必要性，将产品或服务的功能分为核心功能和附加功能，规定了“同意”、“明示同意”、“明示同意+可撤销同意”等不同层级的同意标准。

值得注意的是，由于我国《网络安全法》仅规定了“同意”作为个人信息收集使用的合法事由，因此《个人信息安全规范》并未在“征得授权同意的例外”中考虑企业收集使用个人信息的其他合法事由，而是通过区分不同业务功能的方式，规定企业在收集使用个人信息时所需用户同意的不同标准。

规则点差异	中国个人信息保护规范	GDPR
企业合法利益考量的表现形式	**核心业务功能及所必需收集的个人敏感信息可不逐一获得个人信息主体同意，用户不同意核心业务功能收集个人信息，可拒绝服务。但核心功能收集个人信息还须征得同意，只是同意的标准降低。在标准的修订稿草案中，进一步明确了基本业务功能和扩展业务功能的区分，在此基础上明确企业不得通过捆绑多项业务功能的方式强迫用户接受个人信息收集请求，并区分基本业务功能、扩展业务功能告知与明示同意的不同义务要求。** 通过主动提供或自动采集方式收集个人敏感信息前，应： 向个人信息主体告知所提供产品或服务的核心业务功能及所必需收集的个人敏感信息，并明确告知拒绝提供或拒绝同意将带来的影响。应允许个人信息主体选择是否提供或同意自动采集； 2) 产品或服务如提供其他附加功能，需要收集个人敏感信息时，收集前应向个人信息主体逐一说明个人敏感信息为完成何种附加功能所必需，并允许个人信息主体逐项选择是否提供或同意自动采集个人敏感信息。当个人信息主体拒绝时，可不提供相应的附加功能，但不应以此为理由停止提供核心业务功能，并应保障相应的服务质量。	**数据处理的合法事由中包括：**数据控制者或第三方的合法利益所必须，除非对数据主体的数据利益的保护应高于该等利益；必须在欧盟法或成员国法中明确规定。**此事由并非基于用户同意。** （GDPR 第 6 条）

3、GDPR 规定了更丰富的数据主体权利

除了普遍认可的数据主体知情权、同意权等数据主体权利之外，GDPR 还讲备受争议的被遗忘权和数据可携带权纳入数据主体权利体系。《个人信息安全规范》虽然也规定了个人主体查询、更正、删除个人信息的权利，但与 GDPR 的理想化规定相比进行了一定限缩，更加务实。针对个人信息的被遗忘权，《个人信息安全规范》一是限定了删除个人信息适用的情形是违反法律规定和双方约定收集使用个人信息，或者在个人账户注销后须对个人信息进行删除或匿名化处理。二是为了满足法律法规规定的留存记录及其他的存档记录和统计需求，《个人信息安全规范》规定的“删除”是指在实现日常业务功能所涉及的系统中去除个人

信息的行为，使其保持不可被检索、访问的状态。针对个人信息可携带权，《个人信息安全规范》仅要求在技术可行的前提下直接将个人基本资料、个人身份信息、个人健康生理信息、个人教育工作信息的副本传输给第三方。

规则点差异	中国个人信息保护规范	GDPR
被遗忘权	**仅基于违法和违法双方约定删除：**个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；（《网安法》第 43 条） 3.9 删除　delete：在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。 7.6　个人信息删除（（基于违法和违法双方约定删除） 对个人信息控制者的要求包括： a) 符合以下情形的，个人信息主体要求删除的，应及时删除个人信息： 1) 个人信息控制者违反法律法规规定，收集、使用个人信息的； 2) 个人信息控制者违反了与个人信息主体的约定，收集、使用个人信息的。 b) 个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除； c) 个人信息控制者违反法律法规规定或与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。 **个人信息主体注销账户 （GDPR 没有此要求）** 对个人信息控制者的要求包括： a) 通过注册账户提供服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且该方法应简便易操作；	**该数据之于其收集、处理目的不再必要；** 用户撤回其同意，并且没有其他正当理由支持继续处理该数据； 用户反对处理其个人数据，并且没有其他正当理由支持继续处理该数据，或者出于直接营销目的处理个人数据，遭到用户反对的； 非法处理个人数据的； 为了遵守企业在欧盟或者成员国法律之下的义务，必须删除该数据； 为提供信息社会服务，经其监护人同意而处理儿童个人数据的。 上述规定适用于已经公开的个人数据；此时，企业应当采取合理措施，删除个人数据的链接、复制件等。遗忘权不是绝对的，需要符合比例原则并与新闻自由、表达自由、商业自由等进行平衡。 不适用被遗忘权的五个例外： 保护表达和信息自由； 履行法律义务； 关涉公共健康等公共利益； 为了档案、统计、历史和科学研究等目的； 其他正当理由和抗辩。（17 条）

	b) 个人信息主体注销账户后，应删除其个人信息或做匿名化处理。（《个人信息安全规范》）	
限制处理权	无	在特定情形下，包括个人数据不准确、非法处理个人数据、处理个人数据已不符合目的等，用户有权限制企业处理其个人数据。（18 条）
数据可携权	**与 GDPR 相比限缩了范围** 第 7.9 条 •根据个人信息主体的请求，应为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下个人信息的副本传输给第三方： 1.个人基本资料、个人身份信息； 2.个人健康生理信息、个人教育工作信息。 （《个人信息安全规范》）	个人有权获得其提供给数据控制者的相关个人数据，且其获得的个人数据应当是结构化的、普遍可使用的和机器可读的。 如果技术可行，数据主体应当有权将个人数据直接从一个控制者传输到另一个控制者。 “可携权”适用的两个限定条件： 仅适用于建立在“用户同意”基础上的数据处理活动； 处理是通过自动化方式完成的。 不能对他人的权利或自由产生负面影响。（第 20 条）
反对权	/	基于其合法利益处理个人数据;基于社会公共利益处理数据；用户有权在特定情况下，随时反对处理其个人数据.数据控制者可以提出正当理由进行抗辩。 若为直接营销目的处理个人数据的，数据主体有权随时反对因为该商业目的处理其个人数据，包括与直接营销有关的数据画像。 一旦用户提出异议，企业就应当停止处理其个人数据。（第 21 条）

免受自动化决策权	**范围比 GDPR 限缩：** 7.10　约束信息系统自动决策 当仅依据信息系统的自动决策而做出显著影响个人信息主体权益的决定时（例如基于用户画像决定个人信用及贷款额度，或将用户画像用于面试筛选），个人信息控制者应向个人信息主体提供申诉方法。	只有当完全基于自动化处理对用户进行画像等决策对用户产生法律效果或者其他类似重大影响时，用户才有权反对。 对于用户与企业之间签订、履行合同之必要； 欧盟或者成员国的法律允许； 基于用户明确同意。（第 21 条）

综上，从总体看中国个人信息保护规则与 GDPR 没有原则性差异，这体现了全球个人信息保护的趋同性要求。但中国个人信息保护规则却对 GDPR 一些有争议或者标准过高的规范要求进行了限缩，更适合中国的数字经济发展需求。对于想要走出去的中国企业来说，需要完成从产品或服务设计中、公司运营管理中融入默认隐私的需求，才能满足 GDPR 的规则要求；而对于已满足 GDPR 合规要求，在经营的组织来讲，可能仅是需要一些隐私政策的文本的改动，即可符合国内的合规要求。

（三）GDPR 与我国法的实质性矛盾

1.数据权利的法律限制问题

GDPR 第 23 条“限制条款”对于通过法律限制数据主体和数据控制者的权利义务设定了严格条件，包括实质要求和形式要求两个方面：

在实质要件方面，GDPR 要求相关法律应符合基本权利和自由的本质，且是民主社会应采取的必要的适当的措施，以维护（a）国家安全；（b）防卫；（c）公共安全；（d）刑事犯罪的预防、调查、侦查、起诉或者刑事处罚的执行，包括对公共安全威胁的防范和预防；（e）一般公共利益的其他重要目标，包括经济或财政利益、公共卫生或社会保障；（f）司法独立与司法程序的保护；（g）违反职业道德规范的预防、调查、侦查和起诉；（h）监督、检查或相关的监管职能：（i）对数据主体或其他人的权利与自由的保护：（j）民事请求权的执行。

在形式要件方面，GDPR 要求任何立法措施均应至少包括如下方面的具体措施：（a）处理的目的或处理的类别；（b）个人数据的分类；（c）限制的范围；（d）防止滥用或非法使用或传输的保障措施；（e）控制者具体情况或控制者类型；（f）存储期限和适用的保障措施，且需要考虑性质、范围和处理的目的或分类；（g）对数据主体权利和自由产生的风险；（h）数据主体被告知限制的权利。

GDPR 的上述规定，是基于“数据权利是一项基本权利”这一共识。早在 2007 年 12 月，欧盟议会、欧盟委员会就颁布了旨在保障欧盟公民权利的《欧盟基本权利宪章》，其第 8 条将“个人数据受保护的权利”明确列入基本的自由权中。2016 年《欧盟数字基本权利宪章》（Charter of Digital Fundamental Rights of the European Union）进一步细化了数据权利的内涵。作为一项基本权利，对数据权利的限制必须以高位阶规范——法律方可作出。

但在中国，尽管《民法总则》第 111 条规定了“个人信息应受法律保护”，但其权利性质仍无定论。在实践中，一方面通过行政法规、部门规章，甚至规范性文件限制数据权利的情形不胜枚举。另一方面，即使通过《网络安全法》等法律加以限制，也大多缺乏形式要件。因此，在企业遵守中国法律、法规、规章、规范性文件而降低个人数据的保护标准或违反其对数据主体的承诺，将难以使用 GDPR 第 23 条作为责任免除的理由，从而面临双重困境。

例：向政府报送个人数据

《网络安全法》第二十八条：“网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。”

《电子商务法》第二十七条：“电子商务平台经营者应当要求申请进入平台销售商品或者提供服务的经营者提交其身份、地址、联系方式、行政许可等真实信息，进行核验、登记，建立登记档案，并定期核验更新。”

《电子商务法》 第二十五条：“有关主管部门依照法律、行政法规的规定要求电子商务经营者提供有关电子商务数据信息的，电子商务经营者应当提供。有关主管部门应当采取必要措施保护电子商务经营者提供的数据信息的安全，并对其中的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。”

例如我国《网络安全法》第 28 条、《电子商务法》第 25 条、第 27 条分别规定了网络运营者、电子商务平台经营者向政府部门的个人数据报送义务。以 GDPR 为参考，上述法律没有明确规定防止滥用或非法使用或传输的保障措施、存储期限和适用的保障措施、对数据主体权利和自由产生的风险以及数据主体被告知限制的权利，有待进一步完善。我们建议后续通过立法合理确定数据报送范围、确立报送数据的合法性原则、比例原则、保密性原则、正当程序原则以及相关法定程序、明确政府相关部门的数据保护义务与责任。

2.数据本地化存储的问题

我国对数据本地化存储的规定主要见于《网络安全法》第三十七条：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。”此外，国务院《征信业管理条例》（2013 年）、卫计委《人口健康信息管理办法（试行）》（2014 年）、中国人民银行《关于银行业金融机构做好个人金融信息保护工作的通知》（2011 年）、国家新闻出版广电总局和工业和信息化部联合发布《网络出版服务管理规定》（2016 年）、交通运输部等部委联合发布的《网络预约出租汽车经营服务管理暂行办法》（2016 年）等，都对数据本地化提出了明确要求。根据上述规定，相关数据的存储、处理、访问都必须在境内进行。

我国数据本地化的要求与 GDPR 的监管要求存在冲突。GDPR 第 58 条“权力”条款赋予了欧盟各监管机构普遍的调查权力，特别是：命令数据控制者和处理者提供监管机构执行任务所需的任何信息；以数据保护审计的方式开展调查；获得所有个人数据的访问路径以及执行任务所必要的信息；获得数据控制者和处理者任何资产的访问路径，包括任何数据处理设备和处理方法。由此，一旦欧盟监管机构向相关中国企业发出上述命令，则其不得不陷入违反我国数据本地化规定的困境。我们建议后续通过立法明确企业对境外监管机构基于执法目的调取我国数据的反馈机制，由相关主管部门作出企业是否应向境外监管机构提供相应数据的决定，避免企业面临双重义务违反，也为未来我国进行跨境数据执法调取的国际谈判与合作提供基础和空间。

3.跨境传输限制的问题

GDPR 第五章“向第三国或国际组织传输个人数据”要求，除少数例外情况，个人数据只允许流入欧盟认可能提供“充分保护”或“适当保护措施”的国际或地区。其中，“充分保护”与否，取决于欧盟的认定和评估，只有第三国的立法、数据保护制度能够提供与 GDPR 相同数据保护水平的国家，才能列入欧盟的“白名单”。“适当保护措施”包括：（a）制定有约束力的企业规则：（b）采用欧盟委员会通过的标准数据保护条款；（c）采用成员国监管当局通过并经欧盟委员会通过的标准数据保护条款；（d）遵守协会、不同类型的控制者、处理者组织编写并经批准的行为准则；（e）经批准的认证和第三国控制者、处理者的承诺。

鉴于中国在短时期内不太可能达到欧盟“充分性认定”的要求，GDRP 对数据跨境传输的限制不可避免地与我国对中国企业及其数据的管辖权发生冲突。对此，GDPR 第 48 条“未被欧盟法律授权的传输或披露”明确规定：“根据第三国法庭或审理委员会的判决和行政机构的决定，要求控制者或处理者传输或披露个人数据的，当且仅当提出要求的第三国与欧盟或成员会存在有效的国际条约且不影响本章规定的其他传输依据时，判决和决定才可以被承认或执行。”我们建议中国政府积极与欧盟委员会进行双边谈判和磋商，通过国际条约协定，尽快实现数据合理有序的跨境传输。

4.数据存储期限的问题

GDPR 第 5 条“与个人数据处理相关的原则”中（e）规定：“允许以数据主体可识别的形式保存数据的时间不得超过数据处理目的之必要。”这一被称为“存储期限必要最短”) (storage limitation)的原则与 GDPR 第 17 条“删除权（被遗忘权）”相结合，构成了数据控制者对数据存储的期限要求。然而，由于中国法律、法规、规章对数据存储期限的强制性要求，个人数据可能被超过处理目的的长期存储，或者无法毫不迟延地回应数据主体删除数据的主张。

例如，我国《网络安全法》第二十一条：“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。”《电子商务法》第三十一条规定：“商品和服务信息、交易信息保存时间自交易完成之日起不少于三年。”《征信业管理条例》第十六条：“征信机构对个人不良信息的保存期限，自不良行为或者事件终止之日起为 5 年；超过 5 年的，应当予以删除。”《网络预约出租汽车经营服务管理暂行办法》二十七条规定：“网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年”。

面对这一问题，我们建议及时进行法规清理，提升法律位阶，立足于公共利益，在坚持保存期限“必要最短”的前提下，统一规定个人数据保存期限。同时，仅在例外情形下，才恰当、合理地设定特殊保存期限。

附件一 隐私声明政策示例

（该隐私声明不应被视为符合 GDPR 要求的范本，企业应根据 GDPR 的具体要求，结合自身业务特点及其实践起草的隐私声明。）

隐私声明

最近更新日期：2017年7月6日。查看更新详情，点击这里。

我们理解您关心您的信息是如何被使用和共享的。非常感谢您相信我们对此事处理的谨慎和敏感。本声明将阐述我们对隐私权保护的政策。**如您访问Amazon.com（本网站），您同意接受本隐私声明中所述做法。**

- 我们采集您的哪些个人信息？
- 什么是Cookies？
- 我们是否会与他人共享所收到的信息？
- 关于我的信息安全？
- 第三方广告商和其他网站链接？
- 我能获取哪些信息？
- 我有哪些选择？
- 是否允许儿童使用本网站？
- 欧盟-美国及瑞士-美国隐私保护
- 使用条件、通知和修订？
- 信息采集实例？

我们采集您的哪些个人信息？

我们从客户得到的信息将帮助我们为客户在本网站的购物提供个性化服务，并且不断提升您在亚马逊的体验。我们采集的信息种类如下：

- **您向我们提供的信息：**我们接收并存储您在我们网站上或以其他任何方式提供给我们的任何信息，点击这里查看信息采集实例。您可以选择不提供某些信息，但是这样可能使您无法使用本网站的许多特色服务。我们使用您提供的信息是为了回应您的要求，为您将来在本网站购物提供个性化服务，改善我们的网站以及与您进行沟通。
- **自动获取的信息：**无论您何时与我们进行沟通，我们接收并储存特定的信息。例如，与其他许多网站一样，我们使用cookies。当您的网络浏览器访问本网站或由我们或代表我们在其它网站上提供的广告及其他内容时，我们将获得某些信息。点击这里查看信息获取实例。
- **手机：**当您下载或使用亚马逊或其子公司开发的应用时，我们可能收到关于您所处位置以及您移动设备的信息，其中包含您设备的特定识别符号。我们可能使用这些信息为您提供基于定位的服务，例如广告、搜索结果以及其它个性化内容。大多数移动设备允许您关闭定位服务。关于如何关闭定位服务的更多信息，请点击这里。
- **电子邮件通讯：**为帮助我们把电子邮件变得更有用途和更有趣味，在您打开来自本网站的电子邮件时，如果您的计算机支持一些功能，我们通常会收到一封关于您已收悉电子邮件的确认。我们也会将我们的客户名单与收到的其它公司的名单进行对比，以避免向我们的客户发送不必要的信息。如果您不希望继续收到我们的电子邮件或其它信函，请调整您的帐户中的客户通讯选项。
- **从其他来源获得的信息：**我们可能从其他来源收到关于您的信息并且将其加入我们的客户信息库。点

击这里查看信息采集实例。

什么是cookies？

- cookies是一种我们传至您设备的特定识别符号，从而使我们的系统能够识别您的设备，并向您提供诸如一键下单、为您推荐商品、在其它网站上的个性化广告（例如由本网站和使用亚马逊支付服务的网站提供内容的联盟网站）以及在您多次访问间隔时保存您的购物车中所选商品的记录等特色服务。
- 多数浏览器上的帮助部分会告诉您怎样防止您的浏览器接受新的cookies、怎样让您的浏览器在您收到一条新cookies时通知您或者怎样彻底关闭cookies。此外，您可以通过改变浏览器附加程序（browser add-ons）的设置，或通过访问其制造商的网页，来关闭或删除浏览器附加程序使用的类似数据（诸如Flash cookies）。cookies能让您充分利用本网站最优秀的特色服务，所以我们建议您将其设置为打开状态。例如，如果您关闭或拒绝接受我们的 cookies, 您将不能使用向您的购物车添加商品、进入结算页面、或者使用您需要登录后才能使用的本网站产品和服务。

我们是否会与他人共享所收到的信息？

客户的信息是我们业务重要的一部分，我们不会将其转卖给他人。我们仅以下述方式与适用本隐私声明或至少提供与本隐私声明同样保护性惯例的本网站控制的子公司分享客户信息。

- **不受我们控制的合作商家：**我们与合作商家有密切的合作。在有些情况下（例如第三方卖家），这些商家在本网站开店或在本网站上作为卖家向您销售商品。在另一些情况下，我们会与一些商家联合开店、提供服务或销售产品。点击这里查看联合品牌和共同销售的示例。您可以辨别您的交易何时会涉及第三方卖家，我们与该第三方卖家共享与交易有关的客户信息。
- **第三方服务提供者：**我们聘请其他公司和个人代表我们履行某些职能。例如：处理订单、投递包裹、发送信函及电子邮件、清除客户名单中的重复信息、分析数据、提供市场营销帮助、提供搜索结果和链接（包括付费搜索名单和链接）、处理信用卡付款事项以及提供客户服务。他们能够接触到为履行其职责所需的客户信息，但不能将此信息用于任何其他目的。
- **促销：**有时我们代表其他商家向所选定的本网站的客户群提供促销活动的服务。在提供此服务时，我们不会向这些商家披露您的姓名和地址。如果您不希望收到这类促销信息，请调整您的帐户中的电子邮件偏好设置。
- **业务转让：**随着我们持续发展业务，我们可能会出售或收购商店、子公司或者业务部门。在这些交易中，客户信息通常是所转让企业资产中的一部分，但这些信息（当然除非客户作出其他同意）仍然受制于转让前已有的任何隐私声明所作出的承诺。虽然可能性不大，但在极端的情况下，如果本网站或其几乎全部资产被收购时，客户信息将是被转让资产的一部分。
- **对本网站和其他人的保护：**为了遵守法律、执行或适用我们的使用条件和其他协议，或者为了保护本网站、我们的用户或其他人的权利及其财产或安全，我们将会披露帐户或其他个人信息。这包括为防止欺诈和减少信用风险而与其他公司和组织交换信息。不过很明显，这并不包括违反本隐私声明中所作的承诺而为获利目的出售、出租、共享或以其它方式披露可识别个人身份的信息。
- **征得您的同意：**除以上规定之外，当有关您的信息有可能披露给第三方时，您将会得到通知，并且您可以选择不与第三方分享此信息。

关于我的信息安全？

- 在信息传输的过程中，我们通过使用网络安全层软件（SSL）对您输入的信息进行加密，从而努力保护您的信息的安全。
- 在确认订单时，我们将只显示您信用卡号码的最后四位数字。当然，我们在处理订单过程中会把完整的信用卡号码传送给相关的信用卡机构。

- 防止他人未经授权使用您的密码或使用您的计算机是非常重要的。因此，您应确保在与他人共用一台计算机时，当您使用完毕后即时退出登录。点击这里查看关于如何退出登录的更多信息。

第三方广告商和其它网站链接？

我们的网站上有第三方广告和对其它网站的链接。关于本网站的第三方广告的更多信息（包括个性化或基于兴趣的广告），请阅读基于兴趣的广告政策。

我能获取哪些信息？

本网站允许您进入与您的账户以及和本网站进行互动有关的信息，这种访问的目的仅限于阅读和在特定情形下更新账户信息。点击这里查看示例，示例内容将随网站的变化而更新。

我有哪些选择？

- 如上所述，您可以选择不提供某些信息，尽管您在采购或者使用本网站的某些特色服务（例如您帐户的个人信息、心愿单、客户评论和亚马逊Prime）时被要求提供信息。
- 您能添加或更新上述"我能获取哪些信息"中所述页面上的某些信息。当您更新信息时，我们通常保留一份原有信息的复件存档。
- 如果您不想收到我们的电子邮件或其它信函，请调整您的电子邮件偏好设置（如果您不想收到我们发送的使用条件和其他法律通知例如本隐私声明，这些声明仍将适用于您对本网站的使用，您有责任阅读它们以获知它们的更新）。
- 如果您不希望我们使用我们收集的个人信息以允许第三方对我们呈现给您的广告推广进行个性化设置，请调整您的广告偏好设置。
- 多数浏览器上的帮助功能会告诉您怎样防止您的浏览器接受新的cookies，怎样让您的浏览器在您收到一条新cookie时通知您或者怎样彻底关闭cookies。此外，您可以通过改变浏览器附加程序（browser add-ons）的设置，或通过访问其制造商的网页，来关闭或删除浏览器附加程序使用的类似数据（诸如Flash cookies）。cookies能让您充分利用本网站最优秀的特色服务，所以我们建议您将其设置为打开状态。例如，如果您关闭或禁止接受我们的 cookies, 就不能向您的购物车添加商品，进入自行结帐程序，或者不能使用您需要登录后才能使用的本网站产品和服务。

是否允许儿童使用本网站？

我们不向儿童销售产品，但我们向成年人销售儿童用品。如果您不满18岁，只有在父母或监护人参与的情况下您才能使用本网站。

《欧盟-美国及瑞士-美国隐私保护》

我们参加了《欧盟-美国及瑞士-美国隐私保护》框架协议。点击这里查看更多信息。

使用条件、通知和修订

如果您选择访问本网站，您的访问和有关隐私的争议将受制于本声明和我们的使用条件，包括对赔偿的限制、争议解决和华盛顿州法律的适用。如果您有任何对本网站上有关隐私问题，请联系我们并作充分描述，我们将尽力解决。

我们的业务时常变化，我们的隐私声明和使用条件也随之变化。我们可能通过电子邮件方式定期提醒您我们的通知及条件，但您应经常登录我们的网站了解近期变更。除另有声明外，现行的隐私政策适用于我们关于您和您的账户的所有信息。我们坚守我们做出的承诺，未经相关客户同意我们不会对我们的政策和惯

例作重大修改以至于降低对客户信息的保护程度。

相关惯例和信息请见

- 使用条件
- 用户论坛
- 社区规则
- 帮助中心
- 最近购买
- 您的个人资料与社区指南

信息采集实例

您提供给我们的信息

您在搜索、购买、张贴、参加竞赛或问卷调查时或者与客户服务部门联系时会提供我们大部分的信息。例如，您在搜索产品、通过本网站或我们的第三方卖家订货时提供信息，在我的帐户（如果向我们购物时您使用不止一个电子邮件地址，您可能有一个以上帐户）或您的个人信息中提供信息，在与我们通过电话、电子邮件或其他方式交流、填写调查问卷或竞赛报名表、使用亚马逊Instant Vedio等服务、编辑心愿单或礼品登记、参加用户论坛或其他社区特别活动、提交及评估评论、使用到货提醒功能（如可下单通知）时，您会提供信息。作为这些行为的结果，您可能向我们提供诸如您的姓名、地址和电话号码、信用卡信息、收货人包括其地址和电话号码、一键下单设置中的人名（包括地址和电话号码）、您的朋友及其他人的邮件地址、给我们的评论和电子邮件内容、个人信息中的自我介绍或照片以及财务信息（包括社会保险与驾照号码）。

自动获取的信息

我们采集和分析信息的例子包括用来把您的计算机或移动设备连接到因特网上的IP地址；登录名称；电子邮件地址；密码；计算机和连接信息（诸如浏览器的类型、版本和时区设置、浏览器插件类型和版本、操作系统和平台；购物历史记录（我们有时将之与其他客户的类似信息结合起来创造网站特色，例如畅销商品）；送到或通过或来自我们网站的完整的URL点击情况（包括日期和时间）；cookie数；您浏览或搜索过的商品和您用来联系我们800热线的电话号码。我们也可以使用浏览器数据，如cookies、Flash cookies（也称Flash当地共享对象）或我们网站上的类似数据，来防止欺诈和其他违法行为。在有些访问中我们可能使用软件工具诸如JavaScript测量和收集用户连接的信息，包括网页响应次数、下载错误、对特定页的访问时间、页面交互信息（诸如滚动、点击和光标停留）以及结束浏览该页所使用的方法。我们也可能收集技术信息帮助我们识别您的设备，防止及诊断欺诈行为。

手机

大多数移动设备允许用户关闭定位功能。多数情况下，这些设置位于设备的设置菜单内。关于特定设备的信息，请点击这里。如您对如何关闭您设备的定位服务有疑问，我们建议您联系您的移动设备运营商或设备生产商。

从其他来源获得的信息

我们从其他来源获得的信息的例子包括从我们的承运商或其他第三方得到的最新的配送和地址信息，这些信息供我们更正我们的记录和易于交付您下一次的订货或者便于与您联系；帐户信息，购买或退货信息，以及通过与我们合作联合品牌业务的或者我们为其提供技术、配送、广告或其他服务的企业获得的页面阅览信息；通过我们的关联企业Alexa Internet提供的网络搜索服务而得到的搜索名词和搜索结果等信息；

搜索结果和链接，包括付费搜索名单（如推广链接）；通过信用机构获取的信用历史信息，我们用其协助防止并检测欺诈，并向特定客户提供某些信贷或财务服务。

联合品牌与共同销售

我们与之合作提供共同或联合品牌产品及其他商品的企业包括Starbucks、OfficeMax、 Verizon Wireless、 Sprint、 T-Mobile、 AT&T、 J&R Electronics、 Eddie Bauer与 Northern Tool + Equipment。

您可以获得的信息

您可以轻易地通过本网站获得的信息包括关于订单的最新信息、可识别的个人信息（包括姓名、电子邮件、密码、通信及个性化广告选项、地址簿、一键下单设置等）、付款设置（包括信用卡信息、促销证明和礼品卡余额）、邮件通知设置（包括到货提醒、送货信息和简讯等）、推荐（包括向您推荐的商品和改善您推荐的商品）、购物清单和礼品登记（包括您的商品评论、推荐、Listmania清单、提醒、个人信息及心愿单）。

中国信息通信研究院安全研究所

地　　址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62305900

传　　真：010-62300264

网　　址：www.caict.ac.cn