数美 NEXTDATA

《通用数据保护条例》解读

出海企业合规指南-欧洲篇

GENERAL DATA PROTECTION
REGULATION

前言

中国的互联网行业在海外不断夯实自己的领先优势。据信通院统计，从价值超过 100 亿美元的数字平台来看，中国和美国仍然保持绝对引领。2020 年，中、美百亿美元以上平台企业数量合计达 64 家，全球占比 84.2%，全球新增的 7 家平台均来自中美。2021 年，TikTok 更是首次取代谷歌，成为全球访问量最多的域名。越来越多的中国企业开始展现自己强大的国际竞争力，鼓舞着万千中国互联网企业进军海外。

另一方面，与互联网行业息息相关的隐私保护和数据合规立法也在不断完善。2018 年 5 月，欧盟最严个人数据保护法规《通用数据保护条例》（GDPR）正式生效，引起广泛关注。此后全球隐私立法按下加速键：2019 年 9 月，新加坡新修订的《个人资料保护条例》正式生效；2019 年 12 月，印度联邦内阁通过了《2019 个人数据保护法》；2020 年 7 月，美国加州正式实施《加州消费者隐私法案》（CCPA），又在 2020 年 11 月通过了 CCPA 的修正案《加州隐私权利法案》（CPRA）；2021 年 11 月，中国开始正式实施《个人信息保护法》。随着各国开始制定各自的隐私保护和数据合规法律，出海企业也有必要随时跟进当地立法进展，根据规定调整隐私政策以及业务方向。

数美数字风控研究院“风控 Law School”专栏聚焦数字风控行业，追踪国内外政策法规最新动态，帮助企业敏锐察觉政策趋势，应对合规风险，为企业数字化转型提供坚实后盾。“风控 Law School”将按照互联网企业出海地区推出“出海企业合规指南”，GDPR 为出海系列的第二册。

声明

本册由数美数字风控研究院（公众号 ID: ishumei2015）制作，版权归数美科技所有。

本册主要采用文献综述、桌面调研、行业访谈等调研方法写成，参考文献、数据引用及其来源均在脚注内标出，图片采集于网络公开信息并标注来源。

本册致力于为读者呈现海外监管法律的全貌，然而受研究方法与参考资料的限制，文内观点仅为读者提供行业参考，并不视为针对企业提供的专业建议。

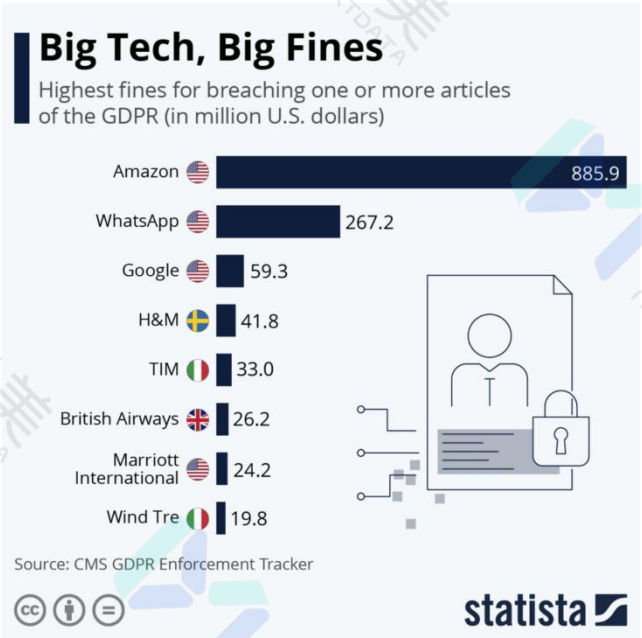
此版为首次发布版本，数美数字风控研究院之后可能会对内容进行再次修订。

目录

一、适用范围

2018 年被称为“世界数据治理元年”。在这一年的 5 月 25 日，《通用数据保护条例》（GDPR）在经过两年的缓冲期后正式步入执法阶段。作为全球首部全面的个人数据保护法，它的出台极大地影响了欧洲乃至全世界的数据保护立法进程。就在 GDPR 正式实施不久，美国加州便匆忙通过了 CCPA 草案，而我国于去年实施的《个人信息保护法》与《数据保护法》在制定过程中也参考了 GDPR 的个人数据保护框架。

除了其在立法上的先锋地位，GDPR 的高额罚金也是其备受瞩目的原因之一。GDPR 生效不到四年，其罚款金额逐年增长：2018 年仅为 43.6 万欧元，2019 年 7200 万欧元，2020 年 1.71 亿欧元，2021 年上涨至惊人的 10 亿欧元。在 GDPR 的罚款名单上不乏多家互联网巨头，截至目前，被罚金额最高的企业是亚马逊。2021 年 7 月，卢森堡的数据监督管理机构以“不遵守一般数据处理规则”为由，向亚马逊收取了 7.46 亿欧元的罚款[1]。



GDPR 罚单金额排行
来源：statista

[1] 数据详见：2022.01.06，DIGIT，“GDPR Fines Totalled over €1bn in 2021”，http://www.digit.fyi/gdpr-fines-totalled-over-e1bn-in-2021/

虽然就现阶段而言，中国互联网企业的主要出海地区是东南亚、中东、北美等地区，但欧盟世界前三的经济体量与较高的消费水平也在不断吸引着中国企业。而欧盟作为发展成熟程度相当高的市场，也通常被认为是海外市场中的高岭之花，获取市场难度高，但一旦成功，能大幅提振品牌信心与国际知名度，TikTok 和 Shein 就是很好的例子。

一方面，出海欧洲的中国企业队伍日益壮大，而另一方面，入局欧洲的准入门槛也越来越高。随着 GDPR 的执法模式日益成熟，企业也迫切需要提升自身的数据保护合规水平，以应对更加制度化的监管。

1.1 立法进程

欧盟的个人数据保护立法大致经过三个阶段：《1981 年个人数据保护公约》（简称“108 公约”）、《1995 年个人数据保护指令》（简称“95 指令”）以及 2018 年《通用数据保护条例》（GDPR）。

108 公约是全球范围内有关数据保护的第一份具有法律约束力的国际文件，其规定，“各方必须在其国内立法中采取必要措施适用其规定的原则，以确保在其领土内尊重所有个人在处理个人数据方面的基本人权”[2]。108 公约原本仅适用于欧盟成员国，在经过数次修订后，也开始面向非欧洲国家及国际组织开放签署。

1995 年，欧盟通过《数据保护指令》，第一次以立法的形式为保护成员国公民个人信息安全设定标准。在 108 公约的基础上，95 指令建立了具有一定可操作性的个人数据保护规则和实施框架，为欧盟成员国的数据保护法令制定了最低标准。95 指令在欧盟立法层级上属于“指令”，不具备直接的执法效力，成员国不能直接照章办事，而应依照指令将其转化为地方法律。由于每个成员国都是按照自己对 95 指令的理解制定地方法律，这也导致各国在保护个人信息的立法进度不一。

2018 年的 GDPR 是对 95 指令的一次提炼与更新，它在生效后直接取

[2] 引用详见：2019.04.06，网络法治国际中心，《国际数据治理：欧洲委员会及其“108 号公约+”》

代了 95 指令。GDPR 作为“条例”，各国的监管机构无需对其进行任何修改转化，可直接依据 GDPR 进行执法。通过提升 GDPR 的立法地位至“条例”，GDPR 成为“一种对其 28 个会员国的 5 亿人甚至其他国家的人，采取一致做法的有效机制。”

1.2 适用范围

GDPR 旨在保护个人隐私权，并加强其对个人数据的控制。GDPR 序言开宗明义地指出，“保护自然人的个人数据处理是一项基本权利”，因此，GDPR 主要聚焦于对“个人数据的处理”。

GDPR 第二条第一款规定，GDPR 适用于所有对于个人数据的使用及处理行为，包括人工处理及自动化处理。

紧随其后，GDPR 列出了不适用的个人数据处理情形：

（1）发生在联盟法律范围之外的活动过程中；

（2）由成员国在欧洲联盟条约第五卷第二章范围内（涉及公共外交与安全政策）进行活动时；

（3）由自然人在纯粹的个人或家庭活动中；

（4）由主管当局为预防、调查、侦查或起诉的刑事犯罪，执行的刑事处罚的目的，包括防范和组织公共安全受到威胁[3]。

除了第二条所列举的，GDPR 另有多处提到其他的不适用情形，如逝者与法人的个人数据处理、经过匿名化处理的个人数据不适用 GDPR。由于 GDPR 力求对个人数据实现最大程度的保护，因此对个人数据的定义非常广泛，而对其他不适用的情形以列举的方式在文内多处列出，此处不一一枚举。但有一点可以肯定的是，以营利为目的的企业所开展的数据处理活动一定适用 GDPR。

由于在不同立法下，“个人数据”的定义也各不相同，因此有必要厘

[3] 原文详见：GDPR Article 2(2)

清在该法中“个人数据”具体指哪些数据。

GDPR 的“个人数据”判断标准为是否可识别，它指任何指向一个已识别或可识别的自然人身份相关的信息，包括姓名、身份证号码、地址信息或网络标识符（包括 IP 地址和 Cookies）等标识，或是物理、生理、遗传、心理、经济、文化或社会身份等要素。

我国的《个人信息保护法》也采用类似的“识别说”。《个人信息保护法》第四条规定：“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。”

加州的 CCPA 则在“识别”的基础上，进一步通过数据与个人的合理关联对个人数据进行限缩，并排除了多种不适用的数据，这也使得 CCPA 定义下的个人数据要比 GDPR 和个保法范围更小。

三部法规对“个人数据”的不同定义也体现了不同的立法理念。GDPR 和个保法的定义较为宽泛，更强调实现最大限度对个人信息的保护，而 CCPA 的个人数据范围相对较小，更有助于数据的无障碍流动，减少数据保护可能给经济增长造成的负作用。

1.3 地域适用范围

GDPR 第三条中规定了其地域适用范围：

（1）本法适用于设立在欧盟内的控制者或处理者对个人数据的处理，无论其处理行为是否发生在欧盟内。

（2）本法适用于对欧盟内的数据主体的个人数据处理，即使控制者和处理者没有设立在欧盟内，其处理行为：

(a)发生在向欧盟内的数据主体提供商品或服务的过程中，无论此项商品或服务是否需要数据主体支付对价；或

(b)是对数据主体发生在欧盟内的行为进行的监控的。

（3）本法适用于设立在欧盟之外，但依据国际公法欧盟成员国法律可适用地的控制者对个人数据的处理[4]。

地域适用范围也是 GDPR 一直以来较大的争议点，其提出的域外管辖权将 GDPR 的适用范围直接延伸至全球范围内任何面向欧盟提供产品、服务、监控的企业。由于 GDPR 原文中并未对地域适用范围作出具体的阐述，监管机构以及企业在实际操作过程中难以判断其是否适用 GDPR，于是，2018 年 11 月 23 日，GDPR 最高监管机构欧洲数据保护委员会（EDPB）发布《关于 GDPR 地域管辖的指引——公众版本》，对 GDPR 地域适用范围的划定作出了具体指引。

判断企业数据处理业务是否受 GDPR 管辖需要关注两点：1. 企业是否在欧盟境内设立实体；2. 若企业实体设立在欧盟外，其是否以面向欧盟提供商品、服务或以监控为目的。

先说第一点。在此种情况下，如何判断企业是否在欧盟境内设立实体？欧盟境内设立的子公司或分公司是否适用？

EDPB 在指引中指出，具有法人资格的分公司、子公司及办事机构均有可能适用 GDPR，前提是“通过稳定的组织进行有效、真实的营业活动”。例如，一家美国汽车制造公司在布鲁塞尔设有办事处，负责其在欧洲的营销和广告活动，那么它可以被视为一个稳定的组织在承担真实有效的营业活动，因此这家办事机构便适用 GDPR。

2021 年 7 月，荷兰数据保护局以侵犯儿童隐私为由，对 TikTok 处以 75 万欧元的罚款，这也是中国企业首次因违反 GDPR 而受到处罚。在案件审理过程中，TikTok 以其主要机构位于爱尔兰为由提出异议。但荷兰数据保护官认为，TikTok 是在调查开展期间才将总部转移至爱尔兰，在爱尔兰的人力与资源尚不足以支持其在当地开展营业活动，反而有借在爱尔兰设立机构为由规避荷兰执法的嫌疑。这一案例也充分说明，GDPR 的地域适用及监管机构认定会结合具体的业务形态判定，而不会局限于实体的设立地点。

[4] 原文详见：GDPR Article 3

再来看第二点，这里的关键在于企业是否面向欧盟境内的人提供产品、服务或监测行为。开发海外专用 APP、使用欧元或欧盟成员国货币结算、使用欧盟域名等均会被判定为向欧盟境内的的个人提供产品或服务。而监控在 GDPR 中的含义进一步延展为包 Cookies、个性化广告推荐、用户画像等监测行为。

1.4 合规建议

GDPR 的主要目的是“通过‘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。”欧盟法律要求成员国当局之间开展合作并进行个人数据交换，且不能以个人数据保护为由限制数据在欧盟境内的自由传输，GDPR 的出台无疑会提升欧盟在数据经济领域的实力。然而，GDPR 对非欧盟国家的企业运营的牵制也尤为明显，高标准的合规要求无疑会大幅提升企业的运营成本，企业需要决定是在短期内承担更高的合规成本以获得准入，还是直接放弃欧盟市场。

二、个人权利

GDPR 的推出对数字时代个人数据保护具有重要意义，它赋予数据主体七项数据权利，极大地保障了个人对其数据的控制权。GDPR 第三章规定，数据主体享有的七项数据权利分别是：访问权、更正权、删除权（“被遗忘权”）、限制处理权、可携带权、反对权，以及不受制于自动化决策的权利。

2.1 访问权

GDPR 第 15 条规定，数据主体有权要求数据控制者告知其个人数据是否正在被处理；如果是，数据主体有权获取其个人信息以及以下相关信息：

（1）处理目的；

（2）正在处理的数据类别；

（3）将接收其数据的第三方或第三方的类别，尤其是位于欧盟以外的第三方或国际组织；

（4）如果有的话，须告知数据的预估存储期限；如果没有，也应告知用户影响存储期限的决定因素；

（5）告知用户拥有更正权、被遗忘权、限制处理权、反对权；

（6）用户有权向监管机构投诉；

（7）如果个人数据不是从数据主体处收集，应告知数据来源；

（8）告知其数据将被用于自动化决策，以及有关自动化决策逻辑的有用信息、决策的重要性及预估后果[5]。

GDPR规定，如果个人数据被传输到欧盟以外的第三国或“国际组织”，数据主体有权被告知与这一传输有关的现行保障措施。

[5] 原文详见：GDPR Article 15（1）

数据控制者应免费提供一份正在处理的个人数据的副本。如果数据主体索要多份副本，数据控制者可以按照管理成本收取合理费用。如果数据主体通过电子方式提出请求，数据应当以常用的电子形式提供。

2.2 更正权

GDPR 第 16 条规定，“数据主体有权要求控制者对其不准确的个人数据做出更正，并不得无故拖延。考虑到处理目的，数据主体有权要求将不完整的个人数据补充完整，包括以提供补充说明的方式”[6]。

简言之，用户可在两种情况下要求企业更正个人数据：1）数据不准确；2）数据不完整。 在收到用户提交的更正数据请求后，企业应及时响应，在收到用户请求一个月之内完成更正。此外，GDPR 也规定，企业不仅有义务配合用户进行个人数据的更正处理，还必须及时通知用户具体的更正情况。如果拒绝用户的更正请求，也应告知拒绝理由。

如果企业与第三方共享该用户的个人信息，企业也应通知第三方做出相应的信息更正。

2.3 删除权（“被遗忘权”）

删除权也被称作“被遗忘权”，它起源于 2014 年欧盟法院的一则判决。2010 年，西班牙公民冈萨雷斯向西班牙数据保护机构 SDPA 提出申请，希望删除谷歌搜索引擎上有关他的负面信息。1998 年，西班牙公民冈萨雷斯因无力偿还债务被没收房产，拍卖广告被刊登在《先锋报》上。2010 年，此时冈萨雷斯已还清债务，但他发现，如果在谷歌搜索他的名字，会出现指向《先锋报》报道的链接。冈萨雷斯认为，由于这些信息不再有相关性，希望可以删除报道和谷歌链接。2014 年，历经四年裁决，欧盟法院支持冈萨雷斯保护其被遗忘权的诉讼请求，这也使之成为欧盟被遗忘权第一案。

[6] 原文详见：GDPR Article 16

GDPR 第 17 条规定，数据主体有权要求控制者及时删除其个人数据，控制者有义务及时删除个人数据，不得无故拖延。但删除权并非任何情况下都可使用，GDPR 对删除权的行使条件也作出了明确的规定，必须满足以下情形：

（1）当个人数据不再为收集或处理它们的用途所需时；

（2）数据主体撤回了同意，并且没有其他合法理由再进行处理时

（3）如果数据主体基于其合法权益对处理提出反对，且控制者无任何优先于其利益诉求的处理法律依据时；

（4）根据控制者对欧盟或其成员国的法律义务，控制者必须删除数据时；

（5）收集的数据是用于“信息社会服务”时；

（6）当数据被非法处理而违反条例时[7]。

同时，GDPR 也进一步限制了删除权的行使条件：

（1）为了保护言论自由和信息自由；

（2）为遵从欧盟或其成员国的法律义务；

（3）基于公共卫生的理由；

（4）为归档、科学或历史研究；

（5）为提出、行使或维护法律主张[8]。

必须要注意的是，完全删除以电子信息形式存储的数据是有困难的，因此企业应确保拥有合适的存储系统来响应用户的删除请求。即使无法删除用户个人数据，企业也应至少采取措施确保该用户数据不会再被处理。

[7] 原文详见：GDPR Article 17（1）
[8] 原文详见：GDPR Article 17（3）

谷歌删除权页面
来源：谷歌

2.4 限制处理权

GDPR 第 18 条规定，只有在以下四种情形下，用户才有权限制企业处理其个人数据：

（1）数据不准确。数据主体对个人数据的准确性提出质疑，因此限制其处理，直到控制者能够证实其准确性；

（2）数据处理非法。对该数据的处理属于非法，但数据主体不希望其数据被删除，而是要求对其使用做出限制；

（3）需作为证据留存。对于控制者的处理目的来说不再需要此个人数据，但数据主体要求保留该数据以用于提出、行使和维护其法律主张（这一情况可能要求从事某些行业的控制者保留以往客户的记录）；

（4）企业其他合法主张。个人依据其反对权，反对对其数据进行处理。在控制者寻求继续处理的合法理由时可使用该限制[9]。

[9] 原文详见：GDPR Article 18(1)

企业可以采取一些方法来响应用户的限制处理请求。例如，可以暂时将该用户数据迁移至另一套处理系统中，使该用户数据无法被用户获取，或者暂时从网站上撤下相关数据。

2.5 可携带权

GDPR 第 20 条规定，“数据主体应有权以结构化的、常用的和机器可读的格式接收其提供给控制者的个人数据，并有权将这些数据传递给另一个控制者，而不受提供此个人数据的控制者的阻碍”[10]。

用户行使数据可携带权需满足两个前提条件。

首先，必须是征得用户同意后采集的数据，如勾选《用户协议》便视作与数据控制者达成协议，同意其收集数据。要注意的是，控制者基于公共利益、政府授权以及履行法定义务等取得的用户数据，不属于可携带数据的范畴，比如政府因疫情防控需要获取的居民行程信息。

其次，必须是以自动化方式采集的数据。也就是说，用户通过提交纸质材料提交的个人数据不属于可携带数据的范畴。

相比于备受争议的被遗忘权，可携带权在全球范围内的接受度要高得多。美国加州的 CCPA 和我国的《个人信息保护法》也都将数据可携带权列为数据主体享有的权利之一，国内多家互联网产品也开始支持导出个人信息。可携带权的落地也将有助于数据流动，发挥更大价值。

[10] 原文详见：GDPR Article 20（1）

微信个人信息导出页面
来源：微信

2.6 拒绝权

GDPR 第 21 条规定，数据主体有权拒绝控制者处理其个人数据。当出现这种情况时，必须暂停处理活动，或由控制者来证明其“处理的法律依据较之数据主体的利益、权利和自由优先，或其处理是为了提出、行使或维护有关的法律主张”[11]。

GDPR 列举了三种拒绝权的适用情形：基于科学研究或统计目的的数据处理的场景、基于直接营销的目的、用于提供信息社会服务。

2.7 不受制于自动化决策的权利

GDPR 第 22 条规定，“数据主体有权不受仅基于自动化决策所做决定的影响，包括那些会对他们产生法律效力或类似重大影响的特征分析”[12]。

自动化决策是指利用计算机技术、算法程序、深度学习或神经网络替代人类处理关键数据，并自动生成决策的行为。当一个决定完全依靠自动化决策来完成，且这个决定可能会对该用户带来法律效力时，用户有权免受其限制。

[11] 原文详见：GDPR Article 21（1）
[12] 原文详见：GDPR Article 22（1）

GDPR 也列出三种可以使用自动化决策的情形：

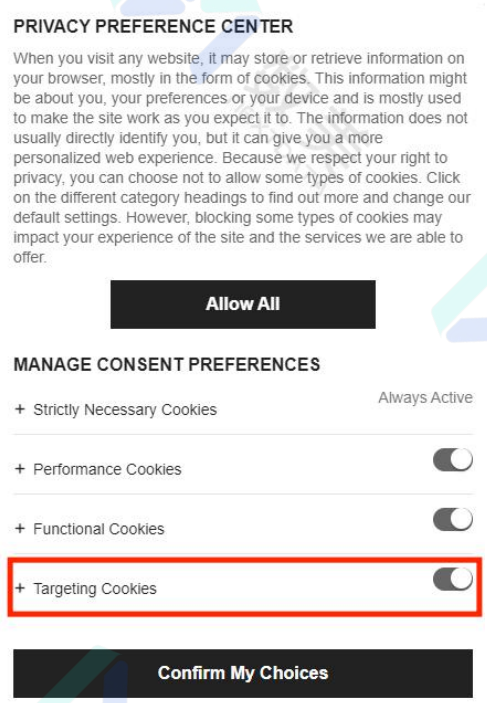
（1）有欧盟或其他成员国某项法律的授权；

（2）数据主体与控制者之间签订合同；

（3）个人明确表示了同意[13]。

但是，在任何情况下，自动化决策应配有相应的保障措施，确保把潜在的风险因素考虑在内，避免对用户的权益造成损失。例如，用户应有权干预相关决策和发表观点，在得到自动化决策评估后应得到解释，且有权质疑这一决策。

以某购物网站的 Cookies 偏好选择为例，用户在首次进入网站时便会出现 Cookies 设置弹窗，用户可自主选择是否同意网站将收集到的个人信息用于自动化推荐等业务。



某购物网站上设置 Cookies 偏好选项
来源：Shein

[13] 原文详见：GDPR Article 22（2）

2.8 合规建议

每个数据主体都有权向监管机构投诉。根据违反 GDPR 的严重程度，企业会被判处不同等级的罚款金额，侵犯数据主体的权利被认为是严重违规行为，可能会导致 2000 万欧元或 4%全球年营业额的最高行政处罚。出海企业应充分理解 GDPR 赋予数据主体的权利，并采取相应的组织手段和技术手段确保数据主体权利不受侵犯。

三、跨境传输

对国际贸易和国际合作而言，与欧盟以外的国家之间的数据流动是不可或缺的，但日益增多的数据跨境流动也给个人数据保护带来了新的挑战与顾虑。当数据在欧盟与非欧盟国家间流动时，也应接受欧盟内同等力度的保护。GDPR 规定，在任何情况下，向第三国或国际组织传输数据必须要满足相关规定。

3.1 跨境传输的定义

GDPR 专设第五章，对个人数据向第三国或者国际组织的传输规则展开了细致的描述，即大家所熟知的数据跨境传输（一般认为“第三国 third countries”指非欧盟条约缔约国的国家）。

2021 年 11 月，欧盟数据保护机构 EDPB 还通过了《Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR》，通过具体的案例分析帮助各成员国更好地理解 GDPR 的跨境传输规则，解决执法过程中的实际适用问题。

总的来说，数据传输行为需同时满足以下三个条件才可认定为 GDPR 中所说的“数据跨境传输”，缺一不可：

（1）数据输出方（控制者或处理者）的处理活动受 GDPR 管辖。是否适用 GDPR 可参照 GDPR 系列解读一——适用范围篇判断。

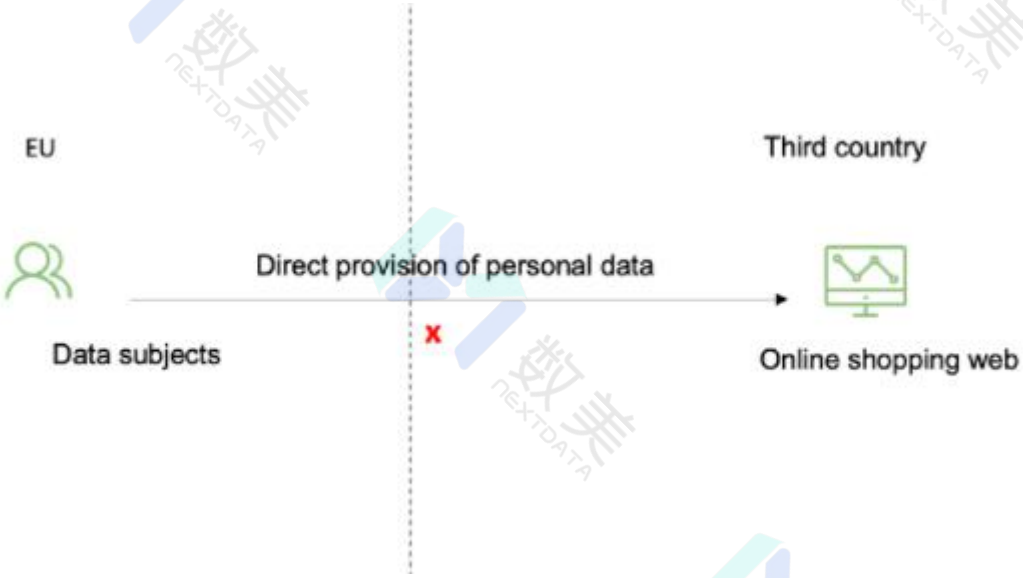
（2）数据输出方通过传输等方式将该数据处理活动项下的个人数据提供给数据接收方。数据接收方包括控制者、联合控制者、处理者等，他们的角色视在数据处理活动中的分工而定。

（3）“数据接收方”位于第三国或是国际组织，无论该境外接收方是否域外适用 GDPR[14]。

[14] 引用详见：Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Chapter 2

根据以上三个条件，位于第三国的数据控制者直接从欧盟内的用户处收集数据，此类的数据收集行为并不属于跨境传输，因为这是数据主体基于个人意愿主动向境外运营商提供个人信息。

例如，意大利用户 A 在新加坡购物网站 B 上购物，在提交订单时提交了自己的电话、地址、银行账户等个人数据。在此种情况下，由于 A 的个人信息是自己自愿提交给新加坡公司 B，而没有通过任何数据输出方，因此该数据传输行为不属于跨境传输，此类数据传输行为无需通过任何额外的审核认定。



GDPR 下的数据跨境传输规则
来源：数据法盟

那么位于欧盟境内的子公司将数据分享给位于第三国的母公司，是否属于跨境传输呢？在此种情形下，子公司被认为是位于欧盟境内的数据控制者，接收数据的母公司则被视为数据处理者，此类数据共享行为也被认为符合数据跨境传输的规定，适用 GDPR 第五章的情形。

有一种数据传输场景对中国企业也较为常见。中国企业 A 未在欧盟境内设立经营实体，其收集的个人数据均为非欧盟居民，因此 A 并不受 GDPR 的管辖。但在经营活动中，中国企业 A 将其数据交给欧盟企业 B 进行处理，欧盟企业 B 再将处理完毕的数据传输给中国企业 A。在此种情况下，由于

欧盟企业 B 的数据处理活动受 GDPR 管辖，因此将数据回传给中国企业 A 仍属于数据跨境传输。

3.2 数据跨境传输需要满足哪些条件？

GDPR 规定，向非欧盟国家传输个人数据应在以下两个特定条件下进行：传输目的地获得欧盟委员会的充分性认定（Transfers on the basis of an adequacy decision），或者，该数据传输行为得到了适当的保障。

1. 充分性认定

当传输目的地已通过欧盟委员会的充分性认定后，欧盟国家向其传输数据无需获取额外授权，遵守 GDPR 对数据传输的普通规定即可。充分性认定要求第三国或国际组织具备以下条件：

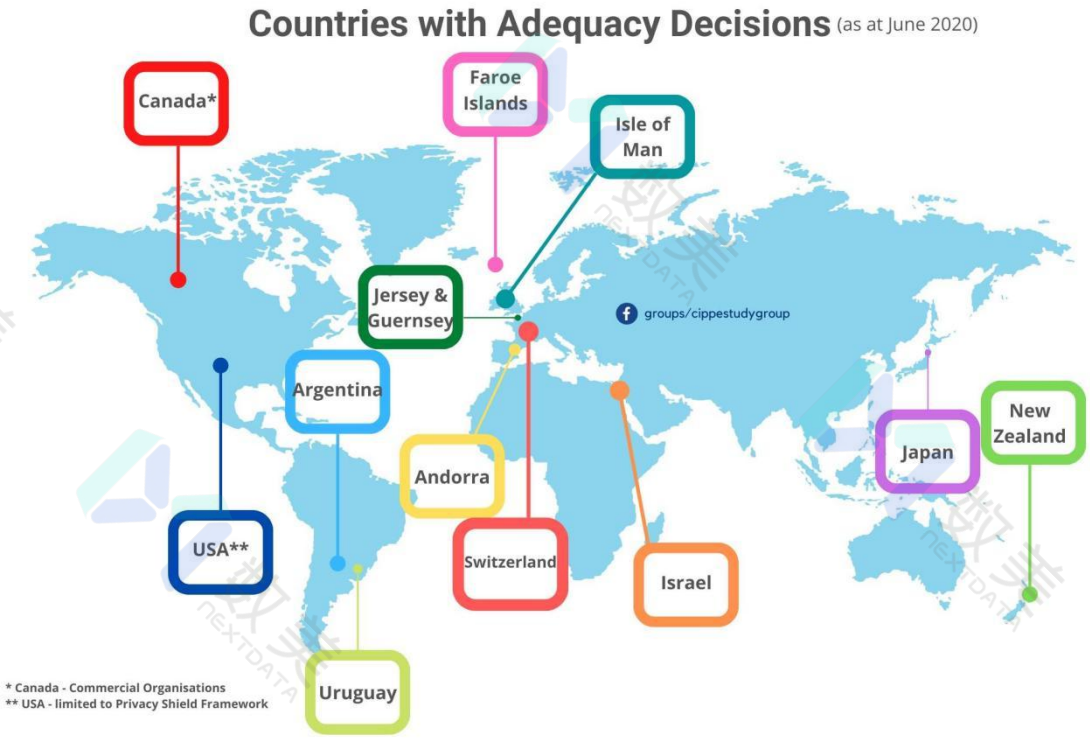
（1）法治，尊重人权和基本自由，相关立法和执法情况；

（2）第三国或国际组织所在国是否拥有负责数据保护的独立监管机构；

（3）第三国或国际组织缔结的国际承诺、有法律效力的公约或文书、加入的与数据保护相关的多边关系或区域体系[15]。

欧盟委员会将按照以上标准进行充分性认定，且每四年进行一次审查，得到充分性认定的国家会在《欧盟官方公报》和欧盟委员会网站上公布。目前达到充分性认定标准的国家有：安道尔、根西岛、泽西岛、阿根廷、以色列、新西兰、加拿大、马恩岛、瑞士、法罗群岛、日本以及乌拉圭。

[15] 原文详见：GDPR Article 45(2)



已获得欧盟 GDPR 充分性认定的国家与地区

来源：Privacy Study Groups

2. 保障措施

获得欧盟充分性认定的国家毕竟是少数。当传输目的地没有获得充分性认定，但能够提供适当的措施来保护数据主体的权利和自由，且数据主体可以申请法律救济，那么向其传输数据也是被允许的。这些保障措施包括以下八项：

（1）公共当局或机构之间有具备法律约束力和执行力的文书。

（2）约束性企业规则。

（3）欧盟委员会通过的标准数据保护条款。

（4）监管机构通过并经欧盟委员会核准的标准数据保护条款。

（5）经核准的行为守则，以及具有约束力和执行力的由第三国控制者/处理者给出的采取适当保障措施和保护数据主体权利的承诺。

（6）经核准的认证机制，以及具有约束力和执行力的由第三国控制者/处理者给出的采取适当保障措施和保护数据主体权利的承诺。

（7）控制者/处理者与第三国或国际组织的控制者/处理者/接收者之间的合同条款。

（8）在公共当局或机构间的行政安排中加入的规定中，包括可执行和有效的数据主体权利[16]。

目前企业传输数据较为常见的保障措施是约束性企业规则（BCR）和标准合同条款（SCC）。

约束性企业规则主要适用多组织或跨国企业在其体系内传输个人数据。标准合同条款被认为是欧盟个人数据出境的主要路径，是经欧盟委员会核准的条款，企业不得随意更改。大多数中国企业都会选择签署 SCC 作为跨境传输数据的有效保障。

3.3 跨境传输的特殊情况

如果传输目的地既未通过欧盟委员会的充分性认定，也无法采取以上提到的保障措施，只有在满足以下条件时，才可向第三国或国际组织传输个人数据：

（1）传输不是重复性的。

（2）只涉及有限数量的数据主体。

（3）对于控制者实现其所诉求的令人信服的合法利益确属必要，且这些利益不会因数据主体的权益或权力与自由而否决。

（4）控制者已评估与数据传输有关的所有情况，并根据该评估为个人数据的保护提供了适当的保障[17]。

[16] 原文详见：GDPR Article 46(2)
[17] 原文详见：GDPR Article 49(2)

也就是说，当数据传输行为是偶发的、必要的，涉及的数据主体较少，并且数据控制者或处理者也采取了适当的保护措施来保障数据安全，此类跨境数据传输无需获得额外的许可。

3.4 合规建议

考虑到实际跨国业务的复杂程度，出海企业应对数据全生命周期中涉及到欧盟的环节格外注意，明确其是否受 GDPR 的跨境传输规则约束。对于确实符合 GDPR 跨境传输定义的业务，跨国公司可考虑采用约束性企业规则、普通的企业可采用标准合同条款，确保数据传输双方都应遵守。

2020 年 7 月，欧盟法院做出 Schrems II 案裁决后，对标准合同条款（SCC）的法律效力又作了进一步说明，明确数据输送双方除了应遵守标准合同条款外，还应核实传输目的地所在国家是否有相应的立法，是否能为传输到该国的个人数据提供 GDPR 所要求的保护力度。这一裁决也使得美国和欧盟之间的隐私盾协议被判无效，多家美国互联网企业与欧盟之间的数据传输业务受到了极大的干扰。GDPR 执法案例的不断更新也迫使企业应持续关注其最新进展。

四、数据处理原则

GDPR 规定，适用 GDPR 的所有数据处理活动均需遵守七项数据处理原则，分别是：（1）公平、透明和合法；（2）目的限制；（3）数据最小化；（4）准确；（5）存储限制；（6）完整与保密；（7）问责与合规。这七项数据处理原则写在 GDPR 的第二章，是 GDPR 隐私保护精神的核心体现，也是企业合规体系的重要组成部分。数据控制者和处理者必须严格遵循这些原则，否则将会构成严重违规行为，可处以 2000 万欧元或 4%全球营业额的最高罚款。

4.1 公平、透明和合法

公平（Fairness）意味着企业的数据处理行为不应损害用户利益，任何含有歧视意味、有误导性或未告知用户的数据处理行为都是不允许的。以反歧视为例，企业如使用 AI 算法处理用户数据，则应配备适当的人工干预，避免算法的自动化操作可能造成的歧视。此外，企业还应定期评估其使用的算法是否会导致歧视、不平等的计算，并做出调整。

透明（Transparency）意味着数据控制者应清楚、公开地告知用户他们打算如何使用已经收集的任何个人数据。用户有权知晓其拥有哪些权利、如何行使这些权利，企业应使用简洁易懂的语言告知用户，必要时可使用视频等可视化渠道向用户解释其中的复杂概念。

合法（Lawfulness）要求企业的数据处理行为必须有合法依据，没有合法依据即为非法处理。GDPR 第六条中列举了数据处理的六项合法事由：

（1）已取得用户同意；

（2）对履行合同是必要的；

（3）对履行法律义务是必要的；

（4）为保护用户或其他人的正当利益；

（5）为公共利益是必要的；

（6）符合企业的正当利益[18]。

对合法依据的判定较为复杂，须结合每一项的实际情况具体分析。以企业的正当利益为例，GDPR 规定，以反欺诈、IT 安全为目的进行的数据处理构成企业的正当利益。此外还应确认，对个人权益的保护是否胜过企业追求的正当利益。

4.2 目的限制

GDPR 规定，企业只能基于“具体、明确及合法的目的”收集个人数据，如果企业的处理目的发生了变化，应第一时间确认新目的是否超出了之前的目的范围。一旦新目的与之前的目的有冲突，企业在重新获取用户同意后，方可继续处理数据。

例如，线上商店 A 为完成订单，需要收集客户的姓名、地址、联系方式等个人信息。商店 A 准备购入一套 CRM 软件，这套软件不仅可以存储客户的个人信息，还可以通过已有数据分析客户的购买力，从而为每位客户提供针对性的广告服务。而这种以个性化广告推荐为目的进行的数据分析已超出最初的目的——完成订单。如果商店 A 希望使用这套软件的所有功能，它应对新的数据处理目的进行评估，明确其是否拥有有效的法律依据，根据评估结果决定是否购入这套软件，或仅使用这套软件的部分功能。

4.3 数据最小化

GDPR 规定，数据控制者所收集或处理的个人数据应“够用、相关且为处理目的所需”。这也就意味着企业应仅收集与其提供的服务相关的个人信息。

[18] 原文详见：GDPR Article 6(1)

数据最小化
来源：Access Now

如果企业希望进一步处理已有数据，应首先判断完成这一处理行为是否可以通过处理更少的数据来完成。如果是的话，企业应删除不必要的数据。此外，假名化、匿名化、集群化等技术可以避免识别到特定数据主体，也可作为实现数据最小化的实现方法。 举例来说，实体书店 B 打算开始经营网店，它需要设立一套表单收集客户订单信息，包括姓名、地址、联系方式等。但实际情况是，并非所有订单需要的个人信息类别都是一样的。如果客户买的是电子书，客户不必提供自己的详细地址。为遵循数据最小化原则，书店应准备两套表单，一套用于向买纸质书的客户，可收集客户的详细地址，另一套则用于买电子书的客户。

4.4 准确

GDPR 第六条第四款规定，个人数据必须“准确且必要时随时更新；考虑到个人数据处理的目的，应采取一切合理措施，确保不正确的个人资料立即被删除或更正”[19]。

不准确的个人数据有可能会对数据主体的权利产生威胁。例如，错误的数据有可能会导致医生做出错误的诊断，这对患者而言很有可能是致命的。

[19] 原文详见：GDPR Article 6(4)

4.5 存储限制

数据在存储时也应遵循最小化原则：不再需要的数据应及时删除，不需要识别个人身份的数据应在假名化、匿名化后再存储。但也有一些例外情况。例如，如果这些数据对公共利益或历史研究有用，数据控制者可继续留存这些数据，并阐述延长存储期限的原因。

与 GDPR 所规定的最短存储期限相比，我国对数据的存储期限则制定了强制性要求，个人数据在处理完毕后可能需要长期储存。《网络安全法》规定，网络运营者应“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”[20]。《电子商务法》也规定，“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”[21]。跨国企业在数据的存储期限上应格外注意。

4.6 完整与保密

GDPR 规定，数据控制者“以确保个人数据适度安全的方式处理，包括使用适当的技术或组织措施来对抗未经授权、非法的处理、意外遗失、灭失或损毁的保护措施”[22]。简言之，企业应采取一定的组织方式或技术手段，确保数据安全，避免发生数据泄露。

4.7 问责与合规

GDPR 第五条第二款规定，“控制者应对遵守第一款中的规定负责，并能做出证明（可问责性）”[23]。尤其在发生数据安全事件时，数据控制者需要提供证据证明，自己已严格遵循以上六条原则，且采用了合适且有效的保护方法，否则需要承担相应的责任。

---

[20] 原文详见：《中华人民共和国网络安全法》第二十一条
[21] 原文详见：《中华人民共和国电子商务法》第三十一条
[22] 原文详见：GDPR Article 5(1)
[23] 原文详见：GDPR Article 5(2)

4.8 合规建议

这七条原则是 GDPR 数据保护合规体系的核心，它们虽然没有规定具体的操作细则，但绝不可忽视它们的指导意义。从实际操作上看，七条原则要求数据控制者对自己的数据处理行为有着足够的风险认知，并采取适当且有效的措施将风险降到最低，这也意味着企业无法套用其他现有的保护措施，必须根据自己的业务情况制定针对性的保护机制，并定期评估是否需要更改。这种以风险为基础的数据保护框架可以最大限度地确保数据安全，保护数据主体权利。

为减少企业的合规负担，欧盟以及国际数据保护机构出台的标准和行为守则也被认为是 GDPR 合规的有效证明。ISO 27001 正是一种与 GDPR 兼容度较高的认证框架，它所提出的应对风险的方法与 GDPR 对影响评估的要求是一致的。通过这些认证虽不能确保企业的数据处理行为完全符合 GDPR，但标准化的框架能证明企业采取了适当的技术和组织手段以预防事故，从而减少企业的举证压力。

五、企业义务

5.1 采取数据保护措施两大原则

GDPR 规定，数据控制者有义务采取适当的技术和组织措施来保护数据主体权利，确保数据处理原则得到贯彻执行，这也是控制者的核心义务。GDPR 并没有要求企业必须实行某项具体的“技术和组织措施”，而是要求这些措施必须是根据数据保护原则而制定，即数据保护设计（Data protection by design）和默认数据保护（Data protection by default）。

原则一：数据保护设计

GDPR 第 25（1）条规定，“考虑到国家的技术发展水平、实施成本和处理行为的性质、范围、环境和目的，以及处理可能给自然人的权利和自由带来的风险和损害，控制者在决定和实施数据处理的方法时，应当以一种有效的方法实施适当的技术、组织措施，例如设计以实施数据保护原则的匿名机制和数据最小化机制，并且将必要的保障措施融入处理中，以使数据处理既符合本条例的要求又保护数据主体的权利”[24]。

简单来说，数据保护设计原则即为“事前提早设计，事中随时调整”。企业在决定数据处理目的时就应考虑如何设计数据保护措施，它不仅对于系统保障用户权利至关重要，也能有效帮助企业降低数据保护成本。数据保护理念要贯穿在数据全生命周期内，要能确保所有个人数据的收集、处理、储存和销毁都要设计成能够保护隐私的一个过程。

除了最开始就要做好顶层设计外，“事中随时调整”也极为重要。由于技术水平、风险、数据处理活动的范围、性质、情境都在不断变化，因此在数据处理活动开始后，企业有必要随时关注最新进展，调整自己的数据保障措施。这也意味着，企业在最初制定保护措施时应注重灵活，以便在遇到更大的风险时能弹性处理。

原则二：默认数据保护

GDPR 第 25（2）条规定，“数据控制者应当实施相应的技术和组织

[24] 原文详见：GDPR Article 25(1)

措施，以确保在默认情形下，被处理的个人数据对于每个特定处理目的都是必要的。该最小必要义务适用于被收集的个人数据的数量、处理规模、存储期限与其可访问性。尤其是这些措施应当确保在默认情形下，个人数据在缺乏个人介入时无法被不特定数量的自然人所访问”[25]。

默认数据保护（或基于默认的数据保护）要求开展任何数据处理活动都应自动采取最有利于隐私的设置，在默认条件下，仅处理目的所需的个人数据。默认数据保护与数据最小化要求息息相关，都要求收集的数据数量、处理程度、存储时间和访问权限必须满足最小必要原则。

此外，企业应当对其数据处理活动做好记录，应包括：

（1）数据控制者及其欧盟代表、数据保护官的姓名、联系方式；

（2）数据处理目的；

（3）对数据主体类型以及个人数据类型的描述；

（4）数据接收方的类别；

（5）跨境传输记录，包括第三国或国际组织的确认以及保障措施记录；

（6）删除不同数据类型的预计期限；

（7）对技术和组织安全措施的一般描述[26]。

5.2 保障个人数据安全

保障个人数据安全也是 GDPR 规定数据控制者应尽的义务之一。GDPR 第 32 条规定，控制者可采取以下措施保障个人数据安全：

（1）个人数据假名化及加密；

（2）确保数据处理系统及服务可持续保持机密性、完整性、可用性及恢复能力；

（3）在发生物理事故或技术事故时，可及时恢复使用、访问个人数据；

[25] 原文详见：GDPR Article 25(2)
[26] 原文详见：GDPR Article 30(1)

（4）定期测试、评估并衡量数据保护技术和组织措施的有效性[27]。

具体来说，企业内部应当建立一套完整的数据泄露处理机制，做到事前规划、提前准备、人员培训、应急处理、事后追责等。

一旦发生个人数据泄露事件，企业应在 72 小时内向数据监管机构报告，并对泄露实际情况、影响以及采取的补救措施进行记录，以供监管机构查询。如果数据泄露事件有可能对数据主体的权利和自由带来高度威胁，控制者也应及时以清晰平时的语言告知数据主体相关情况。

5.3 开展数据保护影响评估

GDPR 第 35 条规定，“为了确保安全，避免处理行为违反 GDPR，控制者或处理者应评估处理过程中的固有风险，并采取措施减轻这些风险，例如加密。在评估数据安全风险时，应考虑处理个人数据所带来的风险，例如被传输、储存的个人数据遭受意外或非法毁坏、遗失、更改、未经授权披露或接触，或以可能导致生理、物质或非物质伤害的其他方式处理”[28]。

数据保护影响评估，简称 DPIA，是数据保护设计和默认数据保护的一个关键部分。DPIA 是企业在开始数据处理活动前就应开始的一项程序，借助它，企业可对处理过程中可能出现的风险进行识别和评估，并采取措施减轻这些风险。DPIA 应至少每三年进行一次。违反规定的，最高可罚 1000 万欧元或高达 2%的全球年营业额。

什么样的企业需要进行 DPIA？一般来说，当一种数据处理方式特别是使用新技术时，如果它可能给数据主体的权利和自由带来高度危险的，数据处理者就应进行 DPIA。尤其当一项数据处理行为涉及以下三种风险因素时，DPIA 就是必不可少的程序：

（1）基于自动化处理的系统而广泛的数据评估；

[27] 原文详见：GDPR Article 32(1)
[28] 原文详见：GDPR Recital 83

（2）大规模地处理特殊类别的数据（可识别某个自然人的数据），或与刑事犯罪和违法行为相关的个人数据；

（3）大规模地系统监视公开区域[29]。

5.4 设立数据保护官

在 GDPR 中，数据保护官（DPO）被认为是数据保护制度中的重要一环。一个组织是否要设立 DPO，应考虑以下三个因素：

（1）由公共机关执行处理，但以司法身份行事的法院除外；

（2）控制者或处理者的核心工作因其性质、范围和/或目的需要对数据主体进行大规模的、定期及有系统的监察的处理；

（3）控制者或处理者的核心活动包括大规模处理特殊类别的数据以及与刑事定罪和犯罪有关的个人数据[30]。

在上述定义中，有两个概念需要着重厘清：“大规模”和“定期及系统的监测”。

GDPR 并未对“大规模”这一概念有着明确的区间范围，这需要企业结合用户数量、数据量、数据范围、处理时间、地理范围等因素综合判断。而像电子邮件营销、位置跟踪这类有预先安排、为企业后续战略执行服务的数据处理活动会被归类为“定期及系统的监测”，这类企业就需要设立 DPO。

对于出海欧洲的中国企业来说，如果在欧洲有稳定的经营实体，DPO 应设立在欧盟境内，以便直接处理 GDPR 合规事宜。

[29] 原文详见：GDPR Article 35(3)
[30] 原文详见：GDPR Article 37(1)

5.5 合规建议

GDPR 的主要目的是保护数据主体权利及自由，这也是企业在开展一切安全措施的重要出发点。企业的数据保护义务与之前的解读文章中所提到的数据主体权利、数据处理原则息息相关，所有这些构成了一个庞大而精密的合规体系。

但同时，由于 GDPR 采用的是以风险为基本的制定方针，为了能更大范围地保护数据主体权益免受侵犯，GDPR 更多提出的是原则性的指导，而非具体的实施手段。这样做的目的是以便企业根据复杂的实际情况灵活处理，从而为用户提供最恰当的保护水平，避免底线思维的存在。但毕竟将原则落实到实践层面还面临不小的困难，近几年不断开出的 GDPR 罚单便能说明问题，这也对企业的合规水平提出了更高的要求。

关于数美科技

数美科技成立于 2015 年 6 月，是一家专业的在线业务风控解决方案提供商，致力于解决在线业务中广泛存在的业务风险与内容风险，为企业数字化转型保驾护航，以两大核心产品：天网——全栈式智能业务风控产品、天净——全栈式智能内容风控产品，推动数字风控行业变革。

数美科技独创全栈式数字风控引擎系统，现已实现全球化 AI SaaS 多集群部署，覆盖中国大陆、欧洲、北美、东南亚、印度等十余个国家和地区，日均风控服务达 30 亿次以上。

目前，数美科技积累了工商银行、银联、小红书、爱奇艺、麦当劳等全球 3000 余家国内外知名企业的服务和客户成功经验，覆盖音视频社交、游戏、银行、新零售、电商、金融等超 15 个行业，被评为企业数字风控行业领军者。

数美科技总部位于北京，并在杭州、上海、深圳、广州设有研发中心和子公司。团队核心成员均来自百度、阿里、腾讯、360、小米等知名互联网企业，拥 10 余年搜索、安全、语音等互联网在线产品研发经验，以及相关领域百余项国家级技术专利。

公司拥有人工智能研究院、黑产研究院、舆情中心、政策研究中心等多个专家服务团队，为客户提供业务风控、内容生态治理相关的技术咨询、解决方案和专业服务，并携手中国信通院、中国科学技术大学等权威机构和院校，成立专项技术实验室，实现产学研用一体化。

公司当前已完成 D 轮融资，由 CPE、经纬中国、厚朴投资、腾讯、襄禾资本等知名机构联合投资。

关于数美数字风控研究院

数美数字风控研究院（公众号 ID: ishumei2015）致力于打造数字风控行业根据地，为从业者带来最前沿的产品、技术、政策解读及深度报告研究。汇聚专业力量，洞悉行业趋势！

数美数字风控研究院

公众号 ID: ishumei2015

数美科技

公众号 ID: ShumeiTech

联系我们

电话：400-610-3866

邮箱：pr@ishumei.com

官网：www.ishumei.com