Baker McKenzie.

Robert Half®

protiviti®
Face the Future with Confidence
甫瀚

· · · 常见问题解答

解读《通用数据保护条例》

欧盟《通用数据保护条例》要求企业必须重点保护个人数据而非控制企业流程，毫无疑问的，这将打破企业现有的安全和隐私程序。

前言

《通用数据保护条例》（GDPR）终于颁布——对于与欧盟居民开展商业活动的企业而言，许多的问题、担忧和挑战亦随之而来。我们将在这里提供一些解读。

历经四年的协商，欧盟 GDPR 于 2016 年 4 月 14 日获得通过，并于 2018 年 5 月 25 日正式生效。受该条例约束的企业曾被赋予两年的宽限期，以审阅既有实务和程序，如今时限已至，企业必须遵守 GDPR 项下的每一条条款（参见下文 GDPR 的发展历程）。

GDPR 有两个高层级的目标：协同欧盟各成员国分散的立法现状；及提升公众对互联网业务固有风险的认知。大量曝光的网络犯罪成功盗取个人数据，引发一众担忧。随着移动设备的爆发式增长、大数据分析的广泛应用，以及通过数字化手段所生产、处理和共享的个人数据的日益增多，当今的个人身份信息面临史无前例的高风险。如何让线上环境变得更加可靠、和谐，是 GDPR 的第一要旨。

GDPR 要求企业必须重点保护个人数据而非控制企业流程，这将打破企业现有的安全和隐私保护程序。GDPR 的内容无疑是广泛的、细致入微的，同时包括多处开放性条款予以企业诠释空间。企业在解读和应对该条例时存在不少疑问。作为回应，贝克·麦坚时、罗致恒富及甫瀚咨询联合推出了该资源指南，针对此项新条例的诸多方面进行了探讨。

请注意，本文所提供的信息并不构成任何法律层面的分析或意见，亦非旨在应对 GDPR 每一领域或其他的数据隐私要求。企业应视其自身特殊情况就特定问题寻求法律顾问或其他领域顾问的意见。

GDPR 发展历程

- 1995 年 10 月：《数据保护指令》（95/46/EC）获得采纳。GDPR 大多数条款都与该指令相同或相似。因此，可以说我们已与 GDPR 的大部分条款相识 20 多年。
- 2012 年 1 月：GDPR 初稿发布。
- 2014 年 3 月：欧洲议会表决支持 GDPR。
- 2015 年 12 月：“三方会谈”（欧盟委员会、欧洲议会和欧盟部长理事会）就 GDPR 达成一致。
- 2016 年 4 月：欧洲议会和欧盟理事会正式采纳 GDPR，并给予两年执行宽限期。
- 2018 年 5 月：GDPR 自 5 月 25 日起开始执行。

目录

GDPR 之洞见

01 什么是欧盟《通用数据保护条例》？

欧盟《通用数据保护条例》是一项泛欧数据保护法，历经欧盟不同机构和成员国多年激烈谈判后于 2016 年 5 月获得通过。该条例旨在强化个体对个人数据的权利，以令数据保护措施匹配数字化时代。

GDPR 于 2018 年 5 月 25 日正式生效，并立即作为欧盟所有成员国的法律强制执行，目标是在 2018 年 6 月将其纳入欧洲经济区协定（EEA Agreement）。

02 GDPR 代替了哪项立法?

GDPR 取代了 1995 年的《欧盟数据保护指令》，及旨在实施该指令的成员国的大部分现行国家之数据保护立法（根据该指令，每个成员国都需要通过国家立法实施该指令）。

03 是否需通过国家立法来实施 GDPR ?

由于 GDPR 本身就是一项管理规定，故无需另行立法来实施。GDPR 将直接适用于整个欧盟。然而，GDPR 包含许多所谓开放式条款，给予了成员国充分的空间来填补 GDPR 的若干领域（例如雇佣情境下的数据保护）。因此，预计每个成员国都将颁布本国法律来对 GDPR 进行补充。截至 2018 年 5 月，只有德国和奥地利颁布了这样的法律。

04 GDPR 适用的地域范围是什么？（第 3 条）

GDPR 适用的地域范围非常广。它不仅适用于设立在欧盟境内的数据控制者和数据处理者对个人数据的处理，而且，即使数据控制者和数据处理者并不设立于欧盟境内，但只要其处理活动涉及向欧盟境内的数据主体提供商品或服务，或监控这些数据主体的行为，GDPR 亦同样适用。事实上，只要其商品或服务的目标群包括欧盟境内的个人，位于欧盟以外的任何企业都有可能受到 GDPR 的监管。

05 GDPR 如何定义个人数据？（第 4 条）

个人数据被定义为与已识别或可识别自然人（“数据主体”）有关的任何信息。可识别自然人能够被直接或间接地识别，尤其是可通过参照诸如姓名、身份证号、定位数据，或在线身份等身份识别信息；也可通过参照该自然人的物理、生理、遗传、心理、经济、文化或社会身份等一个或多个特定要素进行识别。

GDPR 的适用范围非常广。它适用于设立在欧盟境内的数据控制者和数据处理者对个人数据的处理。此外，只要其商品或服务的目标群包括欧盟境内的个人，位于欧盟以外的任何企业都有可能受到 GDPR 的监管。

06 在线身份识别信息是个人数据吗？（第 30 条鉴于条款）

IP 地址、缓存文件和射频识别标签都是潜在的在线身份识别信息。身处数字化时代，数据主体与其使用的设备、应用、工具以及通信协议之间的联系越来越紧密。如果将这些在线身份识别信息与指向唯一的身份识别信息，以及服务器所接收到的其他信息合并起来，就可以用来创建数据主体画像并识别它们。在这种情况下，上述这些在线识别信息符合 GDPR 所规定的个人数据。

07 什么是“敏感”个人数据？（第 9 条）

GDPR 将敏感个人数据称为“特殊类别的个人数据”，包括揭示种族或民族出身、政治观点、宗教或哲学信仰（或信仰缺失）、工会会员资格、健康，或者自然人性生活或性取向的个人信息。这些类别与《数据保护指令》所规定的大致相同。有一个重要点，如果“遗传数据”和“生物识别数据”是被用做唯一识别有关自然人的情况下，那么它们也属于 GDPR 项下的特殊类别个人信息。敏感数据需要接受更为严格的保护，因为对这些数据的处理会大大增加个人权利和自由方面所面临风险的可能性和严重性。

08 有关刑事定罪 / 判决的记录是否被列为“特殊”个人数据？（第 10 条）

与刑事定罪和犯罪有关的个人数据不属于 GDPR 项下的“特殊类别”个人数据。然而，根据 GDPR 的规定，对该等数据的处理须遵守特殊限制条款，其与处理特殊类别数据的适用条款相类似。此外，对该种类别数据的处理必须在政府机关的控制下进行，或经由欧盟或成员国法律授权，该等法律将确保向数据主体提供适当保障。

09 什么是数据主体？

根据 GDPR 的规定，数据主体是指“在”欧洲联盟的任何自然人。该自然人不一定是欧盟的公民或居民，因此，只要对有关个人数据的收集发生在其滞留欧盟领土期间，即使是处理探访欧盟的个人数据，也将受到 GDPR 的约束。我们等待有关当局就“在欧洲联盟”的具体意义给出进一步指引和解释。

10 什么是数据保护原则？（第 5 条）

GDPR 的核心是一套有关处理个人数据的基本原则。这些原则并非最新规定，但 GDPR 现在明确要求数据控制者能够证明其遵守了这些原则（即“问责”）：

- **合法、公正和透明** — 数据的处理对于数据主体而言必须合法、公正和透明。
- **目的限制** — 数据收集目的必须明确、合法并详细说明，且后续处理不得违反以上目的。
- **数据最小化** — 数据必须充分、相关且仅限于达到处理目的所必需之范围。
- **准确性** — 必须及时删除或纠正不准确的数据。
- **存储 / 保留限制** — 可用于识别数据主体形式的数据，其存储期限不得长于处理个人数据所必需的时间。
- **完整性和保密性** — 必须确保以适当安全的方式来处理数据。

11 什么是数据保护设计和默认？（第 25 条）

GDPR 从设计和默认的角度编纂由来已久的数据保护概念，并将其转化为数据控制者需要履行的隐私义务。

数据保护设计意味着，应当从最早期的开发阶段就将数据保护保障措施嵌入有关服务、产品、系统或流程的具体设计中，而非事后才予以考虑。对于可能会用到个人数据的任何新服务、业务流程或 IT 系统，GDPR 要求数据控制者在其整个生命周期都要考虑数据保护的问题。 根据第 25 条规定，数据控制者必须：

- 采取适当的技术和组织措施，有效地实施数据保护原则（例如数据最小化）。
- 将必要的保障措施纳入其处理流程，以满足 GDPR 的要求和保护数据主体的权利。

这些规定非常模糊，以至于在特定情形下什么样的措施合适也需依赖于现有技术和实施成本，以及有关处理所带来的风险结果。

数据保护默认意味着，适当的安全 / 隐私设置必须自动应用于任何数据处理。例如，用户无需对设置进行手动配置更改来提高产品 / 服务的安全性，因为隐私友好默认设置早已到位。此外，默认情况下，

个人数据的存储时限（即“存储限制”）必须仅为提供有关商品 / 服务所必需的时间。企业不应使用预选框。

12 数据处理何时合法？（第6条）

根据 GDPR 的规定，数据处理通常是被禁止的，这与《指令》相一致。数据处理只有在至少满足下列条件之一的情况下才视为合法：

- 数据主体**同意**为一个或多个特定目的处理其个人数据。
- 数据处理是出于**履行合同**的需要（数据主体为该合同中的一方），或是应数据主体请求在订立合同之前采取有关措施所必需的。
- 数据处理是出于数据控制者**履行其不可推卸的法律义务**的需要。
- 数据处理是出于保护数据主体或另一自然人**重大利益**的需要。
- 数据处理是出于执行**符合公共利益的任务**或行使数据控制者被授予的**公务职权**的需要。
- 数据处理是出于数据控制者或第三方寻求**合法利益**的需要，但若需要通过保护其个人数据才能确立的数据主体利益，或是其基本权利超越了上述的合法利益，则将排除在外，尤其是在数据主体为儿童的情况下。

请注意以上内容适用于普通或一般个人数据，对**敏感个人数据**的处理，有关要求更为严格。

13 同意条款的条件是什么？（第7条）

虽然 GDPR 保留了我们所知晓的《数据保护指令》中的同意条款的概念，但总体而言，用获取同意作为处理数据正当理由的这一做法在 GDPR 规定中变得更加困难。如果符合 GDPR 的规定，那么《指令》中所规定的同意条款将继续有效。GDPR 项下所规定的数据主体同意条款是指，数据主体通过声明或明确肯定的举动，所自由做出的、特定的、知情的且非模棱两可的表明其同意处理个人数据的意愿。简言之：

- **非模棱两可的**同意，是指数据主体须做出明确肯定的行为，这就意味着如果选择沉默、同意预选框和不作为的选项将不再视为有效同意。这或许是 GDPR 带来的有关同意条款的最重大的改变。
- **自由做出的**同意，是指数据主体须拥有名副其实的、自由的选择权，并且必须能够在不受到任何损害的情况下随时拒绝或撤回同意。如果数据主体和数据控制者之间存在明显的不平衡，同意就无法自由地做出。
- **特定的**同意，是指必须与特定的处理操作有关，这就意味着如果是非特定处理操作所做出的宽泛同意可能会是无效的。此外同意还必须涵盖进行数据处理所涉及的所有目的，这要求数据控制者须提前决定并明确这些目的。
- **知情的**同意，是指为确保数据主体了解所同意的事实内容和范围，数据控制者必须向其提供足够的信息。同时，数据主体必须至少知晓数据控制者的身份和相关数据处理的目的。

尽管通常情况下口头同意已足够，但仍强烈建议企业获取书面形式（包括电子格式）的同意，毕竟以确凿的证据来证实自己已获得了同意是数据控制者的义务。

如果同意被用来确保敏感数据处理、数据画像或跨境传输的合法性，那么有关同意就需要“明确”。“明确的同意”是何含义还需从监管机构的解释和指引中寻找，并且依赖于获取同意的具体情境。

14 处理未成年人个人数据是否须获得父母同意？（第8条）

将年龄低于 16 岁儿童的个人数据用于提供在线服务时，须首先获得其父母的同意。各成员国可以将获得同意的合法年龄降低，但不得低于 13 岁。

15 GDPR 是否适用于雇佣情境下的数据处理？（第 88 条）

是的，作为一般性规则，它是适用的。然而，GDPR 授权欧盟成员国可以就雇佣情境下对员工个人数据的处理订立更具体的规则。因此，每个成员国都可以针对雇佣情境下的数据处理制定自己的规则，跨国雇主需注意到这一点。总体而言，欧盟的雇佣法并不统一。

16 GDPR对技术有什么要求？

尽管 GDPR 要求企业采取恰当的技术和措施来保护个人数据的安全，但有关措施的性质取决于负责实施的人员。

17 非欧盟企业如何实施GDPR?

GDPR 针对数据向欧盟以外地区的转移做出了明确的规定。其中一项规定便是要求有关转移必须仅面向数据保护法律健全的国家。欧盟并未将美国列为符合该项规定的国家之一。

对于希望接收GDPR监管的个人数据的美国企业，他们可以参考欧盟和美国已达成一致的名为《隐私盾》（Privacy Shield）的系统，美国联邦贸易委员会负责执行该系统。隐私盾的设计旨在创建一项计划，参与其中的企业将被视为拥有充分的保护措施，因此能够支持信息的转移。简言之，隐私盾令美国企业或与美国企业开展合作的欧盟企业能够满足 GDPR 的此项规定。

虽然 GDPR 保留了我们所知晓的《数据保护指令》中的同意条款的概念，但总体而言，用获取同意作为处理数据正当理由的做法在 GDPR 规定中变得更加困难。

18 什么是欧洲数据保护监管机构?

欧洲数据保护监管机构（EDPS）是一个独立的监管机关，其主要目标是确保欧洲各大机构和机关在处理个人数据和制定新政策时尊重隐私和数据保护权。

19 什么是欧洲数据保护委员会?

欧洲数据保护委员会（EDPB）取代了根据 1995 年《指令》第 29 条所成立的工作组（WP29）。其主要角色是推动 GDPR 在各成员国的一致适用和促进各国国家监管机构之间的合作。委员会亦刊发指引和建议。第 70 条条款详细列出了欧洲数据保护委员会的具体职责。欧洲数据保护委员会具有法律人格，由各成员国国家监管机构负责人和欧洲数据保护监管机构负责人或其代表组成。

20 GDPR 如何与 GAPP 协调一致？

《一般公认隐私原则》（GAPP）是一套美国和加拿大用来协助管理隐私政策和程序的框架，适用本土、国家和国际层面。会计师和其他专业人员需要应对许多不同的隐私管理规定和法律。GAPP 可作为一个综合框架，为诸多行业的有效隐私计划提供指导。GAPP 将继续提供有用指引。

21 GDPR 合规审计是否须由欧盟隐私权力机构来执行?

监管机构可以先发制人主动进入企业对其进行评估，确保企业符合 GDPR 的要求；或者监管机构因企业出现个人数据违规行为而进入企业进行调查。监管机构将寻找企业董事会对 GDPR 和个人数据风险有所认识的证据。监管机构需要确保企业已经评估了 GDPR 在企业内的覆盖范围。GDPR 是一个基于风险的监管框架，企业有权根据风险特征选择恰当的控制措施，但前提是，当监管机构上门查访时，他们能够就这些控制做出合理解释。

22 GDPR合规进程中的“基石”是什么?

GDPR 合规最重要的一点就是执行要严格。没有严格的执行，GDPR 合规战略将形同虚设。如果缺乏恰当的运作，并不去培养致力于保护数据的企业文化，即使再完美的政策和员工指南亦毫无价值可言。

23 GDPR合规会如何影响企业对其他法规的合规操作?

这个问题比较复杂。除了GDPR，受此条例约束的企业还必须遵守世界范围内其他众多法规，内容涵盖信息安全、数据隐私、违规通知和文件归档等。这包括（仅举几例）：《支付卡行业数据安全标准》（PCI-DSS）、美国《萨班斯—奥克斯利法案》（SOX）、《美国健康保险携带和责任法案》（HIPAA），以及金融服务行业要遵守的《支付服务指令》第二版（PSD2）、《金融工具市场指令II》（MiFID II），以及世界其他辖区推出的各种反洗钱法规。这些法规对数据的收集、使用和存储，以及企业在发生安全违规时应采取的步骤，均有不同要求。

尽管 GDPR 并非要妨碍为遵守某项法律合规义务所必需的数据处理行为，但 GDPR 与该等以及其他法规之间无疑会存在冲突和不同的规定。企业需要咨询其法律顾问和其他专家，以评估其当前的合规实践，并判断如何才能实现对所有须遵守法规的合规，包括 GDPR。

数据主体的权利

24 哪些信息必须提供给数据主体？（第12-14条）

必须谨记，在欧洲，确保数据主体的个人数据安全是一项基本人权。因此，GDPR的一个主要目标，便是提高数据处理的透明度和强化数据主体的权利。秉承此精神，第13和第14条列出了长长的数据控制者需要提供给数据主体的信息清单。第13条适用于直接从数据主体处收集数据的情况，第14条则适用于从其他渠道获取数据的情况。虽然并非所有信息项目都是新加的，但清单显然要比《指令》及成员国立法所覆盖的范围要广。数据控制者须提供给数据主体的信息包括：

- 有关数据控制者的信息
- 数据保护官的详细联络方式（如适用）
- 数据处理的预期目的和有关处理的法律依据。
- 数据披露的对象或对象类别
- 有关任何预期跨境数据传输的具体细节
- 数据存储时限
- 数据主体的各种权利（例如访问权、删除权和数据可携带权、反对某些处理的权利、撤回同意的权利，以及向监管机构提出申诉的权利）
- 提供个人数据是法定要求还是合同要求，抑或订立合同的必需条件
- 数据主体是否有义务提供数据及未能提供数据的潜在后果
- 任何自动化决策的存在、所涉及的逻辑，以及该等处理会带给数据主体的潜在后果

25 提供给数据主体的信息必须以何种方式传达？（第12条）

信息必须以一种简洁、透明、易懂和易获取的方式提供（免费）给数据主体，且需使用清楚、平实的语言。一般情况下，有关信息必须以书面或电子形式提供。

如有要求，企业必须能够提供电子形式的数据主体记录复本。如果可能，数据控制者还应当能够通过安全系统提供远程访问。

26 什么是个体访问权？（第15条）

第 15 条赋予了个体权利，让其可以从数据控制者处确认数据主体的个人数据是否正在被处理。如果答案是肯定的，那么个体有权访问有关数据并获知下列信息：

- 有关处理的目的
- 所涉个人数据的类别。
- 数据用于对外披露的接收对象，及有关该等数据跨境传输的任何信息
- 数据的存储时限或至少提供确定存储时限的标准

- 数据主体拥有要求纠正或删除其个人数据的权利及限制或反对处理的权利
- 数据主体向监管机构提出申诉的权利。
- 个人数据并非从数据主体处收集的情况下，关于其来源的任何信息
- 自动化决策的存在、所涉及的逻辑，以及该等处理可能带给数据主体的后果及重大意义

如有要求，企业必须能够提供电子形式的数据主体记录复本。如果可能，数据控制者还应当能够通过安全系统提供远程访问（第 63 条鉴于条款）。如果数据主体提出要求，有关信息可以通过口头形式提供。

如果数据控制者有合理理由对信息请求人员的身份提出质疑，那么数据控制者可以要求有关人员提供额外的必要信息来确认其身份。

如果他人的权利和自由（例如知识产权、商业秘密或受版权保护的软件）与数据主体的访问权冲突，那么数据控制者或许有义务拒绝给予若干访问权（第 63 条鉴于条款）。此外，如果所处理的有关数据主体的数据数量庞大，数据控制者可以缩小请求访问的范围。

27 什么是纠正权？（第16条）

数据主体有权要求数据控制者及时纠正其不准确的个人数据。他们亦有权要求将其不完整的个人数据补充完整。

28 什么是删除权？（第17条）

第 17 条赋予了个体在下列情形下要求删除或清除其个人数据的权利（除若干例外）：

- 就收集或处理数据的目的而言，有关数据已非必要。
- 数据主体撤回了处理其数据所依据的同意，且不存在可以依赖的其他法律处理其数据的依据。
- 数据主体依法反对有关处理。
- 有关数据被非法处理。
- 为遵守欧盟或成员国法律规定的法定义务必须对数据进行删除。
- 数据收集与向儿童提供信息社会服务有关。

提请注意的是，在下列情形下，上述删除条款不再适用：

- 企业 / 组织因行使言论自由权而需持有的个人数据。
- 因遵守某项法定义务而需持有的有关数据。
- 因公众利益原因而持有的数据（例如，公众健康、科学、统计或历史研究目的）。

只要数据主体提出有关要求，数据控制者就必须在不会造成延误的情况下删除其个人信息，并终止与第三方分享。如数据控制者已将个人数据公开，则必须在考虑现有技术和成本后，采取合理的步骤，将删除要求通知到正在处理该等数据的其他数据控制者，以确保他们删除该等数据的任何复本或链接。此项“删除权”虽然也被称为“被遗忘权”，但它不能与欧盟法院在“谷歌西班牙与冈萨雷斯”一案中所确立的被遗忘权相提并论。

29 什么是限制处理权？（第18条）

数据主体在下列情形下有权限制对个人数据的处理：

- 数据主体对数据的准确性提出质疑及数据控制者正在核实有关准确性时。
- 数据处理不合法，但数据主体不建议删除数据，而是要求有限制地使用有关数据。
- 数据控制者基于处理目的已不再需要有关数据，但数据主体因法律诉求却需要有关数据。
- 数据主体反对有关处理，其需要核实数据控制者能否依赖令人信服的合法理由后，来决定是否继续有关处理。

在限制处理适用情形下，数据控制者可以存储有关数据，但不得再以任何其他方式进行数据处理，除非获得数据主体的同意，或处理数据的目的是用以提出、行使或捍卫法律的诉求，或出于重要的公众利益原因。

GDPR 本身并不禁止“数据画像”，相反，只要存在法律依据（例如同意或合法利益）及个体并不提出有效反对，数据画像是被允许的。如果数据画像被用于直接营销目的，则个体对此行为拥有反对权。

30 数据控制者是否须通知他人有关数据的纠正或删除或处理限制？（第19条）

是的，数据控制者必须就个人数据做出的任何纠正或删除或处理限制告知个人数据已披露的接收对象，除非这一行为被证明不可能实现或需付出不合比例的工作量。

31 什么是数据可携带权？（第20条）

数据主体有权以一种结构化的、通用的及可机读的格式从数据控制者那里接收个人数据，并且有权将该等数据传输至另一数据控制者而不受最初获得该等数据的控制者的妨碍。若技术可行，数据主体有权将个人数据直接从一个数据控制者处传输至另一控制者。数据可携带权仅适用于通过自动化手段处理的情况及基于同意或合同的情况。

如行使数据可携带权会对他人的权利和自由产生不良影响，则该权利将会受到限制。GDPR 鼓励数据控制者开发可交互操作格式以提高数据的便携性，但控制者并无义务采纳技术兼容的处理系统。

32 什么是反对权？（第21条）

数据主体有权反对在若干情形下对其数据的处理，包括：

- 用于直接营销目的的数据处理。
- 以数据控制者或第三方权益为目的的数据处理。

反对权对于直接营销环境绝对适用，即该项权利一旦被行使，数据控制者就必须立即停止以直接营销为目的的数据处理。同样，在上述第二种情形下，数据控制者必须停止有关数据处理，除非控制者能够提出令人信服的、优先于数据主体利益和权利的合法处理依据。

33 关于数据画像和自动化决策，数据主体有哪些权利？（第22条）

数据画像本质上就是一种自动化的数据处理，其中涉及利用个人数据来评估个体的若干特征，例如个人偏好、经济状况、健康状况、兴趣爱好、位置或行踪。通过跟踪网络浏览活动来预测购买行为就是一个常见的例子。

GDPR 本身并不禁止“数据画像”，相反，只要存在法律依据（例如同意或合法利益）及个体并不提出有效反对，数据画像是被允许的。如果数据画像被用于直接营销目的，则个体对此行为拥有反对权；如果数据画像符合合法利益或用于执行符合公众利益的任务或行使公务职权之目的，则个体对此行为拥有有限反对权。

为保护个体，GDPR 规定，当纯粹基于数据画像（或其他自动化处理活动）的决策会对个体产生法律上的后果或类似的重大后果时，个体有权不受相关决定的限制。例如，在没有人为干预的情况下，自动拒绝个体在线上的信用申请或线上招聘是不被允许的。该权利存在若干豁免情形，例如已获得了个体的同意，或者根据数据主体与数据控制者之间所达成或履行的合同，有关决定是必不可少的。

数据控制者和数据处理者

34 什么是数据控制者以及什么是数据处理者？（第4条）

数据控制者决定数据处理的目的和方式。数据处理者则代表数据控制者来处理个人数据。不同于《指令》，GDPR 不仅将隐私合规义务直接强加于数据控制者身上，数据处理者亦被强制履行隐私合规义务。

35 什么是问责原则？（第24条）

GDPR 要求数据控制者采取适当的技术和组织措施，并能够证明数据处理活动符合 GDPR 的规定（“问责”）。每种情况下的适当措施取决于相关处理的性质、范围、内容和目的，以及个体的权利和自由方面的风险。在实践操作中，这项义务复杂繁琐且意义深远，最好通过实施全面隐私管理计划来履行。

36 什么是联合数据控制者？（第26条）

任何一项处理活动，数据控制者都有可能超过一家。当两个或两个以上控制者共同决定处理的方式和目的时，他们就成为了联合数据控制者。根据要求，联合数据控制者须通过一种正式安排的形式，在他们彼此之间分配好数据保护合规责任，并且有关安排必须如实反映他们各自相对于数据主体的角色。而数据主体必须知悉有关安排的主要内容。

37 设立于欧盟之外的数据控制者和数据处理者是否须指定一位代表？（第27条）

如果设立于欧盟以外的数据控制者和处理者将欧盟数据主体列为目标对象，那么他们必须指定一位代表。该代表必须以书面形式指定，并且必须在相关数据主体所在的成员国之一设立。

然而，下列情况下无需委任代表：

- 处理是偶尔发生的，不包括大规模的对特殊类别数据的处理或第 10 条项下对有关刑事定罪和犯罪个人数据的处理；以及考虑到有关处理的性质、内容、范围及目的，不太可能对自然人的权利和自由造成风险的情况；或
- 数据控制者为公共机关或机构。

GDPR为数据处理协议引入了若干重大新规定，这可能会要求大多数数据控制者和数据处理者更新其数据处理协议。

38 代表是否等同于数据保护官？（第27及37条）

否，代表的要求和职责不同于数据保护官。代表本质上是“提供数据处理的代理服务”，可以代替数据控制者或处理者或与两者一起与监管机构或数据主体进行直接的联系。相反，数据保护官（参见问题 48-50）可以是企业内部人员（也可由外部

人员担任），其主要职责是针对数据控制者或处理者于GDPR项下的义务向其提供咨询及合规监督。

39 企业具体哪些行为会被视为向欧盟数据主体“提供商品或服务”？

第 23 条鉴于条款就该问题提供了一些指引，称应确认控制者或处理者向一个或多个成员国提供商品或服务的预期是否明显。单纯能够访问某个网站或电邮地址并不足以确认有关意图。 然而，如果使用了某成员国的常用语言或货币，并且可以将该语言设定为用来订购商品或服务的语言，那么在这种情况下可以认为控制者有意向欧盟数据主体提供商品或服务。下列问题可能对实践操作有所帮助：

- **域名：**您的企业是否有基于欧盟的域名，例如 .de、.fr、.ie 或者 .eu？
- **语言：**您的企业网站是否有，比如，法语或德语版?
- **货币：**您的企业是否提供以欧元或其他欧盟货币计的交易?
- **内容：**您的网站是否载有来自，比如，希腊的个人引荐或推荐?

如果上述任一问题的回答是肯定的，那么 GDPR 可能完全适用于您企业的任何相关数据处理。

40 数据控制者和数据处理者是否须更新其数据处理协议？（第28及29条）

GDPR为数据处理协议引入了若干重大新规定，这可能会要求大多数数据控制者和数据处理者更新其数据处理协议。与《指令》相比，GDPR对协议必须要涵盖的内容的规定性更强。例如，有必要在协议中增加条款，要求处理者协助数据控制者遵守数据泄露通知规定及执行数据保护影响评估。数据控制者亦须要求数据处理者按照合同的规定（根据控制者的指示），在处理服务完成之后删除或返还全部个人数据。此外，数据处理者应当向数据控制者提供所有证明第28条项下合规的必要信息，并允许和配合合规审计。

41 谁须留存处理活动的记录？（第30条）

作为一般性条款，根据 GDPR 的规定，数据控制者和数据处理者（及其代表 < 如适用 >）须留存有关处理活动的详细书面记录并在监管机构要求时出具有关记录，这一点是能够证明 GDPR 合规的重要基础。从积极的角度看，企业将不再需要像大多数成员国以往那样，须根据《指令》定期通知监管机构其数据处理活动。此外，雇佣人数少于 250 人的企业可豁免遵守该义务，除非：

- 有关处理可能会给数据主体的权利和自由造成风险（例如评分、全面监控、使用新技术等）；
- 有关处理并非偶尔发生；或
- 有关处理包含特殊类别数据（参见问题 7）或与刑事定罪和犯罪有关的个人数据（参见问题 8）。

在实践操作中，大量雇佣人数少于 250 人的企业可能仍须留存处理活动的记录。

42 记录处理活动时应当包含哪些信息？（第30条）

有关处理活动的记录必须为书面形式（包括电子形式）且包含详细信息。至于必须记录哪些信息，GDPR 对数据控制者和数据处理者分别做出了规定。我们强烈建议企业参考第 30 条和监管机构公布的指引来准确了解其记录保存义务。广义而言，GDPR 要求必须记录以下信息：

- 数据控制者、数据处理者及任何代表（如适用）的详细信息
- 有关处理的目的
- 数据主体的类别及个人数据的分类
- 接收者的类别
- 有关跨境传输的详情
- 数据存储时限
- 对用来保障个人数据的技术和组织安全措施的描述

43 数据处理须采取哪些安全措施？（第32条）

根据第 32 条条款，为保障个体的权利和自由，数据控制者和数据处理者须根据数据处理中的固有风险，采取适当的技术和组织措施在一定程度上确保与之相匹配的数据的安全。这是一项宽泛的义务，但在实际操作中却须详细评估各种因素，包括数据处理活动的目的、潜在风险、安全现状，以及实施成本等。GDPR 并未明确规定具体的安全

措施，而是高屋建瓴地提供了若干选择，即：

- 假名化或加密
- 根据公认标准和企业风险水平，确保处理系统和服务具备持续保密、可用和快速恢复的能力
- 在发生物理或技术事故的情况下，及时恢复个人数据可用性和可及性的能力
- 对安全措施的有效性进行测试、评估和评价的流程

企业亦可考虑遵守经批准的行为准则或获取认证，两者均可就企业对 GDPR 项下安全规定的合规予以证明。

44 如果发生数据泄露，企业需要做些什么？（第33及34条）

GDPR 为数据控制者引入了数据泄露通知义务，而根据《指令》，以往只有极少数成员国须履行此项义务。遵守此项义务至关重要，如若不合规可能会导致巨额罚款和名誉损失。尽管该项义务仅直接适用于数据控制者，但数据处理者如获悉有关数据泄露，其亦有责任在不造成不当延误的情况下通知数据控制者。

数据泄露被广泛定义为导致所传输、存储或处理的个人信息发生意外的状况，或非法损毁、丢失、篡改、未授权披露或访问的任何安全违规事件。

如发生数据泄露，数据控制者必须：

- 在不造成不当延误的情况下及，如可行，在获悉有关泄露后的 72 小时之内，通知主管监管机构。
- 若有关泄露可能会令数据主体的权利和自由面临高风险，在不造成不当延误的情况下，就有关泄露向受影响的数据主体做出沟通；有限例外情形除外。

在下列情况下无需就数据泄露向受影响的个体做出沟通（但如果数据控制者决定不通知受影响的个体，则应注意确保数据控制者能够证明有关情形）：

- 数据控制者通过实施适当的技术和组织保护措施（例如加密），为相关数据提供了充分的安全保障；
- 泄露发生后，数据控制者已采取措施确保不再可能产生有关数据主体权利和自由的高风险；或
- 通知个体数据主体需付出不成比例的工作量——在这种情况下须通过公开渠道进行披露。

GDPR 在第 33 和 34 条条款中规定了任何数据泄露通知都必须包含的内容（例如有关数据泄露性质的具体信息、泄露可能造成的后果、所采取的风险缓解措施），并且对面向监管机构和受影响主体的通知进行了区分。无论如何，企业都需仔细衡量应在这些通知中披露哪些信息。

GDPR 规定的通知时间非常短，并且要求数据控制者对任何实际或可疑的数据泄露给予迅速和最大程度的关注。但在实际操作中，数据控制者“意识到”有关泄露的时间节点可能并不总是那么一目了然。第 29 条工作组刊发的指引表示，当数据控制者“能够合理确定导致个人数据受损的安全事故已经发生”时，他便意识到了数据泄露。围绕此，该指引进一步指出：

“数据控制者究竟何时可以被认为‘意识到’某泄露事件，取决于该具体泄露事件当时的情形。在有些情况下，从一开始就可以比较清楚地确定已发生泄露；而有些情况，则可能需要一些时间才能确定个人数据是否已经受损。然而，重点应当放在迅速采取行动进行调查来判断个人数据是否真的被泄露，以及如果确定数据确已泄露，须采取补救措施并根据要求做出通知。”

45 什么是数据保护影响评估及何时须执行该评估？（第35条）

数据保护影响评估（DPIA）是一套正规的、系统的流程，用以评估拟进行的数据处理操作对个人数据保护的影响。GDPR 要求企业在特定情形下开展数据保护影响评估，目的在于最大程度地降低可能对数据主体的权利和自由造成的风险。数据控制者在开始进行相关个人数据处理活动之前，应执行此项评估。

GDPR 要求企业在特定情形下开展数据保护影响评估，目的在于最大程度地降低可能对数据主体的权利和自由造成的风险。

当出现“在考虑了有关处理的性质、范围、内容和目的之后，如果某种类型的处理，特别是采用新技术的处理，可能会对自然人的权利和自由造成高风险”的情形时，就必须执行数据保护影响评估。

GDPR 列出了下列须执行数据保护影响评估的几种情形：

- 开展旨在评价数据主体的个性化特征，以建立数据画像为目的的自动化处理及类似活动
- 大规模处理特殊类别数据或与刑事定罪及犯罪有关的数据
- 大规模、系统化监控公共访问领域

监管机构还应当公布须执行数据保护影响评估的处理操作清单。此外，第 29 条工作组就实际操作中何时可能需要执行数据保护影响评估刊发了指引，并且建议只要心存疑问就应执行数据保护影响评估。

46 我应如何执行数据保护影响评估及有关数据保护影响评估的文档必须包括哪些信息？

GDPR 并未规定开展数据保护影响评估须遵循的流程或格式。相反，它意在向数据控制者提供灵活的操作。第 29 条工作组指引（实际操作中应进行咨询以获得更多指南）确认，数据控制者可以选择适合其数据保护影响评估目的的方法论。

然而，GDPR 明确规定数据保护影响评估至少须包含下列内容：

- 对拟进行的处理操作和处理目的的描述
- 对处理必要性和合理性的评估
- 对数据主体权利和自由风险的评估
- 拟实施的用以应对风险和证明 GDPR 合规的措施（包括确保个人数据得到保护的保障、安全措施和机制）

47 如果数据保护影响评估表明数据主体的权利/自由将面临高风险，数据控制者在开始处理之前还必须采取哪些额外措施？（第36条）

如果数据保护影响评估表明在数据控制者缓解措施缺失的情况下，拟进行的数据处理将会导致高风险，那么数据控制者必须在开始数据处理之前咨询主管监管机构。作为咨询流程的一部分，数据控制者必须向监管机构提供详细的信息。作为一般性规则，监管机构必须在接到咨询请求后的八周内（该期限可以延长）做出响应，并确认拟进行的处理是否会违反 GDPR。

48 我的企业是否须指派一名数据保护官？（第37条）

GDPR 规定，在下列情形下，数据控制者和数据处理者须任命一名数据保护官（DPO）：

- 有关处理由公共机关或机构执行，基于司法权进行数据处理的法院除外。
- 数据控制者或处理者的核心活动所包含的处理操作要求对数据主体进行定期和系统的大规模监控。
- 数据控制者或处理者的核心活动包含对特殊类别数据以及有关刑事定罪和犯罪个人数据的大规模处理。

重要的是，除上述规定情形之外，成员国可以制定条款要求企业在其他情形下亦任命数据保护官，因此国家立法也必须予以考虑。仅以举例而言，德国就拥有更严格的规定，因此对于在德国开展核心活动的企业，其必须任命一位数据保护官的可能性就高于比如，总部设于英国的企业。

第 29 条工作组提供下列指引，以帮助企业确定在实际操作中是否必须指派一名数据保护官：

- “核心活动”包括实现业务目标所必需的关键业务活动以及与核心活动密不可分的活动（例如对病人数据进行处理就与医院提供医疗保健的核心活动密不可分）。
- “大规模”应视具体情况而定，需考虑数据主体的人数、数据量及 / 或不同数据项目的范围、处理持续的时间及所覆盖的地域范围。
- “定期监控”被解释为持续发生或在一定期间内按一定间隔发生；在固定时间反复或重复发生；或不断地或周期性地发生。
- “系统监控”指根据系统进行的监控；是预先安排、组织或井然有序的；是数据总收集计划的一部分，或作为战略的一部分被执行。

拥有多家分公司的企业也可以只任命一位数据保护官，只要这位数据保护官可以很方便地联系到。企业可以选择委任一名内部或外部数据保护官。数据保护官必须具备数据保护法和实务方面的专业知识，有能力履行其职责。

49 数据保护官应向谁汇报？（第38条）

数据保护官的独立性必须得到确保，并且数据保护官将直接向企业的“最高管理层”报告。他们不得

因其履行职责而被解雇或受到处罚，并且必须向他们提供履行职责所必需的资源。

50 数据保护官的职责有哪些？（第39条）

数据保护官的职责包括：

- 告知数据控制者 / 处理者及处理数据的员工须根据 GDPR 及其他数据保护法所承担的义务，并提供意见
- 监督企业对 GDPR、其他数据保护法及内部政策的遵守情况，包括人员的责任分配、意识强化和培训，以及相关审计工作
- 应要求就数据保护影响评估提供意见
- 配合监管机构并充当联系人

数据保护官的独立性必须得到确保，并且数据保护官将直接向企业的“最高管理层”报告。

51 如何运用 GDPR 项下的行为准则？（第40条）

GDPR 鼓励制定行为准则，以促进本条例的正确运用。该等行为准则将为不同领域的具体处理情形提供指引和最佳实践。遵守该等行为准则将有助数据控制者和数据处理者证明其对 GDPR 的合规。

GDPR 授权能够代表各类数据控制者或数据处理者的协会及其他机构编制这些准则。准则需要获得监管机构的批准，或当处理活动涉及多个成员国时，获得欧洲数据保护委员会的批准。

GDPR 为行为准则列出了以下内容：

- 公正、透明的处理
- 数据控制者在特定情形下对合法利益的追求
- 个人数据的收集
- 个人数据的假名化
- 向公众和数据主体提供的信息
- 数据主体权利的行使
- 向儿童提供的信息及对儿童的保护，以及获取儿童父母的同意
- 数据控制者的义务，包括隐私设计 / 默认及用以确保安全处理的措施
- 个人数据泄露的通知
- 个人数据向第三国或国际组织的传输
- 用以解决数据控制者和数据主体之间数据处理争端的庭外程序及其他争端解决程序

52 如何执行行为准则合规？（第41条）

对行为准则相关内容拥有一定专业知识并且能够证明其独立性的机构，在经主管监管机构认可后，可以获得对行为准则合规进行监督的权利。数据控制者和数据处理者若被发现未遵循相关准则，将被暂停参与该准则系统并被报告至监管当局。

53 获得认可须满足什么条件？（第41条）

为获得主管监管机构的认可，从而有权对行为准则的合规进行监督，机构必须：

- 证明其独立性及其在准则内容方面的专业性。
- 设置相关程序，允许其评估数据控制者和处理者适用行为准则的资格、监督遵守情况并定期审查准则系统运行情况。
- 设置相关程序和架构，处理针对准则违规，或针对控制者或处理者已经或正在采用的准则实施方式方面的申诉，并须将有关程序和架构对数据主体和公众公开。
- 证明其职责不会导致利益冲突并获得主管监管机构的认可。

54 什么是认证？（第42及43条）

GDPR鼓励各成员国、监管机构、欧洲数据保护委员会和欧盟委员会设立数据保护认证机制以及数据保护印章与标记。认证虽属自愿性质，但它能够令数据控制者和处理者证明其对GDPR的合规，特别是证明了其就适当技术和组织措施予以了实施。认证亦有助数据向欧盟外第三国的传输，因为欧盟境外数据控制者和数据处理者可以依赖这些认证证明其能够提供适当保障。

认证将由获得认可的认证机构或主管监管机构根据已建立的标准予以签发，一旦签发，最长有效期将为三年。在同等条件下，认证可获得续延。但如果认证要求得不到满足，认证将被撤销。

欧洲数据保护委员会负责将所有认证机制以及数据保护标记和印章整理在册，并确保其公开可用。

跨境数据传输

55 跨境数据传输的基本规则是什么?

GDPR 大体保留了《指令》所建立的跨境传输条款。作为一般性规则，个人数据只能从欧盟 / 欧洲经济区输出至被认为能够提供充分数据保护的国家（“充分性决议”）。如果传输者符合特定情形下的豁免，或能够提供确保充分数据保护的额外保障，那么数据也能被传输至其他非欧盟 / 欧洲经济区国家。

56 跨境数据传输的充分性决议是什么?（第45条）

欧盟委员会有权通过签发充分性决议，认定任何欧盟/欧洲经济区以外的指定国家，或该第三国的某一区域或一个或多个特定行业，或某国际组织，能够确保充分的数据保护。而向这些已被赋予充分条件的国家、区域、行业或组织传输数据，如若是监管机构所允许的，则无须进一步获得特别授权。

于本文着笔时，该等“充分”辖区包括安道尔、阿根廷、加拿大（受《个人信息保护及电子文件法案》（PIPEDA）约束的商业企业）、法罗群岛、根西、马恩岛、以色列、泽西、新西兰、瑞士和乌拉圭。日本正争取与欧盟委员会就相互充分性结果达成一致意见。

对于美国，欧盟委员会于 2016 年 7 月对《隐私盾》框架签发了充分性决议。根据《隐私盾》的规定，美国企业可以向美国商务部做出自我核证，并公开承诺遵守该框架下经欧盟委员会认可的在本质上等同于欧盟隐私标准的隐私标准。因此，《隐私盾》能够实现用于商业目的的数据从欧盟向参与《隐私盾》的美国企业的传输。自我核证虽属自愿性质，但企业一旦公开承诺遵守该框架条款，根据美国法律，有关承诺就将变为强制执行。

作为一般性规则，个人数据只能从欧盟 / 欧洲经济区输出至被认为能够提供充分数据保护的国家。

尽管 GDPR 所保留的充分性概念承袭自《指令》，但 GDPR 也带来了一些值得注意的变化，包括:

- 充分性决议不仅可以针对一个国家，也可以针对区域、行业和国际组织。
- 充分性决议将接受定期审核，并且可由欧盟委员会废除、修订或暂停。
- 充分性决议的条件更加严苛。例如，要想获得充分条件，第三国需要确保其数据保护程度在本质上等同于欧盟的保障水准，尤其是必须确保有效的、独立的数据保护监管到位，并且数据主体能够获得有效的、可强制执行的权利，以及有效的行政和司法救济。

对充分性决议更严苛的附加要求源于声名狼藉的 Schrems 决定，该决定直接导致《安全港协议》的失效和《隐私盾》的实施。

57 GDPR规定的适当保障是什么？（第46条）

只有传输者能够提供适当的保障措施，确保充分的数据保护，并且在数据主体可获得其权利可强制执行和有效法律救济的条件下，数据方可从欧盟向不具备充分条件的第三国传输。

GDPR 所规定的适当保障措施包括无须监管机构特别授权的保障和须经有关授权的保障。

下列适当保障措施无须监管机构特别授权：

- 约束性企业规则（参见问题 58）
- 欧盟委员会采用的标准数据保护条款（参见问题 59）
- 获批准的行为准则或获批准的认证机制，并且两种情况下都需要第三国的数据控制者 / 处理者就其采取的适当保障措施做出具有约束力及可强制执行的承诺，包括有关数据主体权利的承诺（参见问题 51-54）
- 公共机关或机构之间具有法律约束力及可强制执行的工具

须经监管机构特别授权的适当保障措施有：

- 控制者或处理者与第三国或国际组织的控制者、处理者或个人数据接收者之间的合同条款
- 在公共机关或机构之间的行政安排中间插入的，包括可强制执行的、有效的数据主体权利在内的规定

58 什么是约束性企业规则？（第47条）

跨国企业为获得集团内部跨境数据传输的合法资格，可以选择拟定和实施一套具有约束力的规则或行为准则，即约束性企业规则（BCRs）。约束性企业规则强制企业设立于欧盟以外的附属企业实施欧盟隐私标准，从而使得这些附属企业能够处理源自欧盟的数据。约束性企业规则无法用于实现向供应商、客户、分销商或服务提供商等非附属机构传输数据的合法化。约束性企业规则的实施相当繁琐，但 GDPR 竭力减轻企业的合规负担。约束性企业规则须获得主管监管机构的批准。

59 什么是标准数据保护条款？（第46条）

标准数据保护条款（亦被称为“示范条款”）是另一种数据保护措施，以实现数据从欧盟向不具备充分条件的第三国安全地传输。示范条款将义务加诸于数据传输者和接收者，以确保传输安排能够保护数据主体的权利和自由。如果数据控制者或数据处理者能够原封不动照搬全部示范条款，他们便可为相关数据传输提供适当保障。

在 GDPR 之前，欧盟委员会就欧盟数据控制者分别向非欧盟数据控制者及非欧盟数据处理者的数据传输发布了标准合同条款。根据 GDPR，这些条款在被正式废除、修订或取代前将继续有效。根据 GDPR，标准数据保护条款可由欧盟委员会采纳或者由监管机构采纳后再获得欧盟委员会的批准。

重要的是，根据 GDPR，数据控制者或数据处理者可以采用其他条款或保障措施来补充经批准的标准合同条款，只要这些条款或保障措施不与经批准的标准合同条款相抵触或损害数据主体的基本权利和自由。标准数据保护条款作为跨境数据传输合法化的手段正受到欧盟法院的质疑。

标准数据保护条款是另一种数据保护措施，以实现数据从欧盟向不具备充分条件的第三国安全地传输。

60 什么是GDPR项下可以依赖的跨境数据传输可豁免情形？（第49条）

如果传输者能够依赖特定豁免情形，即便不具备充分条件，数据传输亦可合法。根据 GDPR，豁免情形有：

- 在被告知因缺乏充分性决议和适当保障措施，有关传输可能会带给数据主体风险之后，数据主体已明确同意所提议的传输。
- 有关传输对于履行数据主体和控制者之间的合同是必要的；或对数据主体于签订合同之前所要求的实施措施是必要的。
- 有关传输对于控制者与另一自然人或法人之间签订或履行符合数据主体利益的合同是必要的。

- 有关传输出于重要的公众利益原因是必要的。
- 有关传输对于提出、行使或捍卫法律诉求是必要的。
- 在数据主体因为身体或法律原因无法给予同意的情况下，有关传输对于保护数据主体或他人的重大利益是必要的。
- 有关传输源自公众登记册，且已满足特定条件。
- 有关传输不重复，仅涉及有限的数据主体，且对于控制者追求并未超越数据主体权益和自由的重大合法利益是必要的；以及对于有关传输，控制者能够提供保护个人数据的适当保障措施，并将相关传输通知监管机构和数据主体的。

最后一项是 GDPR 新引入的豁免情形，应被视为豁免情形的“最后选择”，适用于只涉及少量数据主体、偶尔进行的数据传输的合法化。

监管机构

61 成员国是否仍须根据GDPR设立国家监管机构？（第51条）

是的，每个成员国都必须规定一个或多个独立公众机关负责监督 GDPR 的适用。大多数成员国都将继续维持一个这样的国家监管机构。某些成员国（例如德国）则设有多家监管机构。这些成员国须指定其中一个监管机构，作为这些机构在欧洲数据保护委员会的代表，并须制定一项机制，以确保各家机构在遵守机制相关条款上的一致性（参见问题 66）。

62 哪个监管机构对跨境传输拥有管辖权？（第56条）

每个监管机构在其管辖区内都拥有管辖权。在没有资格限制的情况下，如果数据控制者通过多个营业场所或因其他原因（例如由于数据主体位于不同成员国）从事跨境数据处理，该规则经常会导致多家监管机构对于同一事项均拥有管辖权。为保护控制者和处理者不必应对多家监管机构，第 56 条规定将以数据控制者 / 处理者的主要或唯一营业场所所在地的监管机构作为“主”监管机构，其对有关控制者所开展的跨境处理拥有管辖权。但主监管机构有义务与其他“有关”监管机构开展合作。该等其他有关监管机构是指数据控制者或处理者可能设有营业场所或受影响数据主体所居住的其他国家的监管机构，或收到审诉的监管机构。在实际操作中，主监管机构可能难以确定，企业应当借鉴第 29 条工作组所刊发的指引。

此项跨境处理的规则亦存在重要豁免情形。例如，主监管机构之外的监管机构亦有权处理向其提出的申诉或可能违反 GDPR 的行为，但前提条件是，申诉事项仅与设立于该监管机构所属成员国的营业场所相关；或仅对位于该监管机构所属成员国境内的数据主体产生了重大影响。因此，地方监管机构将有空间辩称，即使他们并非主监管机构，他们亦拥有管辖权。

尽管欧盟委员会最初拟打造一种“一站式”系统，意图让在多个欧盟国家开展业务的企业只需与一家监管机构打交道即可，但在实际操作中，由于欧盟委员会的立法草案在通过过程中引入大量修正，事实情况往往并不是如此。

63 主监管机构与有关监管机构之间的合作规则是什么？（第60-62及66条）

GDPR 针对主监管机构与有关监管机构之间的合作制定了详细的规则，包括规定他们须互相交流信息；有关监管机构须在主监管机构需要时（例如执行调查）向其提供协助；以及主监管机构须就决议草案征求有关监管机构的意见。当主监管机构和有

关监管机构无法就相关事宜达成一致时，相关事宜将提交欧洲数据保护委员会解决。

该合作规则存在紧急例外情形。如有关监管机构有理由认为迫切需要采取行动以保护数据主体的利益（例如数据主体权利的执行可能会受到严重阻碍）时，那么它可以立即采取临时措施以在自己的管辖区内产生法律效力，但这些措施的有效期不超过三个月。

64 分配给监管机构的职责是什么？（第57条）

第 57 条为监管机构列出了长长的职责清单。首当其中的是监督和执行 GDPR 的适用；提高公众对与个人数据处理相关的风险、规则、保障以及权利的认识和理解；处理申诉；鼓励拟定行为准则；及为数据处理操作提供意见。

65 什么是监管机构行动报告？（第59条）

每个监管机构都须针对其活动刊发年度报告，内容可以包括所接收到的违规事项类型清单及所采取的措施类型。这些报告将被公之于众，或许可以为监管机构的执法行为和优先关注事项提供有用洞见。

66 什么是一致性机制？（第63-67条）

为确保 GDPR 在欧盟的一致适用，GDPR 要求各国家监管机构之间相互合作，并在适当时，与欧盟委员会进行合作。通过刊发意见和指引、向欧盟委员会报告以及解决监管机构之间的争端等一系列行为，欧洲数据保护委员会将在促进一致性方面扮演重要角色。此外，监管机构在采纳第 64 条所列措施之前，必须征求欧洲数据保护委员会在某些方面的意见，例如约束性企业规则、标准合同条款或须执行数据保护影响评估的处理操作清单。存在冲突的，欧洲数据保护委员会将拥有最终决定权。

救济、责任和处罚

67 数据主体如何提出申诉？（第77条）

如果数据主体认为对其个人数据的有关处理违反了GDPR，他们有权向监管机构提出申诉。申诉可以向数据主体所居住或工作或涉嫌违反行为发生的成员国监管机构提出。监管机构须在收到有关申诉的 90 天内，通知数据主体申诉的进展情况。

68 数据主体是否也可以启动法院诉讼程序？（第78及79条）

可以。数据主体在不影响其向监管机构提出申诉权利的情况下，如果认为由于对其个人数据的处理违反了 GDPR 而令他们的权利遭到侵犯，那么他们亦有权获得有效的司法救济。该等针对数据控制者或数据处理者的诉讼应向数据控制者或处理者设有营业场所或数据主体常住地所在成员国法院提出。

此外，对于监管机构所做出的具有法律约束力的决议，或者对于监管机构并未处理申诉或并未就有关申诉进度做出适当通知的情形，数据主体有权获得有效司法救济。该等诉讼应向监管机构设立地所在成员国法院提出。

69 数据主体是否能获得违反赔偿？（第82条）

能。任何人因违反 GDPR 的行为而遭受重大或非重大损害的，都有权就所遭受的损害从控制者或处理者处获得赔偿。控制者和处理者都应对所造成的损害承担责任。参与处理的控制者将对违反 GDPR 的处理行为所导致的任何损害承担责任。处理者则仅在其未遵守 GDPR 针对处理者所规定的具体义务，或者超出或违背控制者的合法指令的情况下，方对处理行为所造成的损害承担责任。如果控制者和处理者能够证明他们对引发有关损害的事件并不负有任何责任，那么他们都可以豁免赔偿。

70 是否数据控制者和数据处理者都应担忧GDPR项下的行政罚款和处罚？

GDPR 明确表示，作为一般性规则（为促进 GDPR 条款的执行），不论是作为对强制实施的适当措施的补充抑或替代性措施，都应对违反 GDPR 的任何行为处以惩戒和行政罚款。例外情况包括违反行为性质较轻，以及如果处以罚款会对自然人造成过度负担的情形。在该等情形下，可发布谴责以代替罚款。GDPR 规定了罚款上限和确定罚款数额的标准，主管监管机构将依据个案做出最终决定。

71 如何决定是否要处以罚款，及如果决定罚款，罚款数额又如何确定？（第83条）

作为一般性规则，监管机构必须确保对于每个个案所实施的行政罚款均有效、理所应当且具有惩戒性。第 83 条所列出的清单包含了在确定是否处以罚款及罚款数额时必须要考虑的综合因素，包括：

- 违反行为的性质、严重程度及持续时间
- 违反行为的故意或过失特征
- 所采取的用以减轻所遭受损害的措施
- 控制者 / 处理者的责任程度
- 控制者 / 处理者以往的任何相关违反行为
- 与监管机构的合作程度
- 违反行为所涉及的数据类别
- 监管机构获知违反行为的方式
- 对以往曾就同一事项采取过的纠正性指令的遵守情况
- 对已获批准的行为准则或认证机制的遵守情况
- 与个案相关的可加重 / 减轻违反情节的因素

GDPR 规定了两种级别的罚款。在每种情况下，GDPR 都设定了罚款上限，且由主管监管机构在考虑了上述所列因素后决定每个个案的具体数额。

违反下列条款的将被处以最高 10,00 万欧元的行政罚款，或如若违反主体为企业，则将被处以最高企业上一财年全球年度营业额 2% 的罚款（两项以较高者为准）。

第 8 条 – 关于儿童就信息社会服务做出同意的适用条件

第 11 条 – 无须识别身份的处理

第 25 条 – 数据保护设计和默认

第 26 条 – 联合控制者

第 27 条 – 设立在欧盟之外的控制者或处理者的代表

第 28 条 – 处理者

第 29 条 – 在控制者或处理者的授权下处理

第 30 条 – 处理活动的记录

第 31 条 – 和监管机构的合作

第 32 条 – 处理过程的安全性

第 33 条 – 向监管机构通知个人数据泄露

第 34 条 – 就个人数据泄露向数据主体做出沟通

第 35 条 – 数据保护影响评估

第 36 条 – 事先咨询

第 37 条 – 数据保护官的任命

第 38 条 – 数据保护官的地位

第 39 条 – 数据保护官的职责

第 40 条 – 行为准则

第 41 条 – 对已批准行为准则的监督

第 42 条 – 认证

第 43 条 – 认证机构

违反下列条款的将被处以最高 20,00 万欧元的行政罚款，或如若违反主体为企业，则将被处以最高企业上一财年全球年度营业额 4% 的罚款（两项以较高者为准）。

第 5 条 – 与处理个人数据有关的原则

第 6 条 – 处理的合法性

第 7 条 – 同意条款的条件

第 9 条 – 对特殊类别个人数据的处理

第 10 条 – 对与刑事定罪和犯罪有关的个人数据的处理

第 12 条 – 与数据主体行使权力有关的透明信息、沟通及形式

第 13 条 – 从数据主体处获取个人数据时应提供的信息

第 14 条 – 从非数据主体处获取个人数据时应提供的信息

第 15 条 – 数据主体的访问权

第 16 条 – 纠正权

第 17 条 – 删除权（“被遗忘权”）

第 18 条 – 限制处理权

第 19 条 – 关于个人数据的纠正或删除或处理限制的通知义务

第 20 条 – 数据可携带权

第 21 条 – 反对权

第 22 条 – 自动化个人决策，包括数据画像

第 44 条 – 传输的一般原则

第 45 条 – 基于充分性决议的传输

第 46 条 – 须采取适当保障措施的传输

第 47 条 – 约束性企业规则

第 48 条 – 欧盟法律未授权的传输或披露

第 49 条 – 特定情形下的豁免

第 58 条 – 监管机构的权力

一些特定的处理情形

72 GDPR是否适用于雇佣情境下的数据处理？（第88条）

适用。但第 88 条允许成员国制定更具体的条款，以确保对雇佣情境下的数据提供保护。这意味着每个成员国均可针对雇佣情境下的数据处理制定自己的规则。因此，跨国企业雇主需要了解每个个案并遵守相关国家规则。

GDPR 亦表示，员工对其个人数据处理所做出的同意可能不会有效，因为在自由状态下做出该等同意的可能性不大。

73 GDPR是否限制用于研究目的的数据处理？（第89条）

只要确保适当的保障措施（例如假名化）到位，为科学或历史研究目的而进行的个人数据处理都是被允许的。科学研究的释义范围很广，包括（例如）技术发展和演示、基础研究、应用研究，以及私人资助的研究。

74 GDPR是否优先于专业保密义务？（第90条）

如果控制者或处理者须遵守专业保密义务，那么该义务就可能与监管机构要求的获取数据或进入场地的权利相冲突。GDPR 意识到这一点，因此允许成员国出台具体细则来规范监管机构的权利，进而协调个人数据保护权与保密义务之间的关系。

关于贝克·麦坚时 (BAKER MCKENZIE)

贝克·麦坚时帮助身处全球经济竞争格局中的客户跨越挑战。我们解决复杂的跨境、跨业务领域的法律问题。我们历经 65 年发展起来的独特企业文化，令我们的 13,000 名人员能够了解当地市场和驾驭多个辖区，作为值得信赖的同事和朋友，我们与客户并肩合作，为其注入信心。(www.bakermckenzie.com)

关于罗致恒富 (ROBERT HALF)

罗致恒富成立于 1948 年，是全球首家且规模最大的专业人力资源公司，也是专业咨询与人才配备服务领域的公认领军者。我公司的专业人才配备服务包括：针对会计和财务领域的 Accountemps®、Robert Half® Finance & Accounting 及 Robert Half® Management Resources，三者均涵盖临时、全职及高级项目专业人员的配备；针对高技能办公和行政支持专业人员的 OfficeTeam®；针对信息技术专业人员的 Robert Half® Technology；针对律师、律师助理和法律支持专家以及咨询解决方案的 Robert Half® Legal，该服务涵盖临时、项目及全职人员的配备；以及针对互动、设计、营销、广告和公关专业人员的 The Creative Group®。

罗致恒富亦是甫瀚咨询的母公司。甫瀚咨询是一家全球性的咨询公司，帮助企业解决财务、技术、运营、治理、风险和内部审计领域的问题。欲获取更多信息，包括职业资源与行业调查，请访问 roberthalf.com。

关于甫瀚咨询 (PROTIVITI)

甫瀚咨询是一家全球性的咨询机构，为企业带来精深的专业知识、客观的见解、量身定制的方案和无与伦比的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球20多个国家的70多家分支机构，我们及旗下独立拥有的成员公司为客户提供财务、信息技术、运营、数据、分析、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询为超过60%的财富1000强及35%的全球500强企业提供咨询服务，亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。甫瀚咨询是Robert Half International Inc.（纽约证券交易所代码：RHI）的全资子公司。RHI于1948年成立，为标准普尔500指数的成员公司。

欲获取更多信息，请登录 protiviti.com/GDPR。

甫瀚咨询如何助力企业达致成功

身处业务和技术密不可分的世界，安全性不能再仅被视为业务的附属品。我们的使命是，依托真正的“业务-信息技术”伙伴关系，帮助各行各业的管理者设计不仅能够保护业务并且能够解锁企业收入增长机遇的安全和隐私系统。我们提供全面的安全和隐私评估、架构、转型及管理服务：

- 安全性计划和战略
- 漏洞评估和渗透测试
- 事故应对和法证服务
- 数据安全和隐私管理
- 身份和权限管理
- 网络安全智能应对中心（CIRC）

Baker McKenzie.

bakermckenzie.com

Robert Half®

roberthalf.com

protiviti®

Face the Future with Confidence

甫瀚

protiviti.com / protiviti.cn