白皮书: EXIN 隐私与数据保护 基础与要领

201912 版

关于作者

Leo Besemer
CertiQA
https://www.certiqa.nl/website/
联系方式：leo.besemer@certiqa.nl

版本管理

版本	修订
201707	初始版本
201912	• 因 GDPR 的全面法规化和欧盟数据保护委员会 EDPB 的设立，对相应内容做出修改。 • 删除了从 GDPR 颁布到生效期间有关情形的段落。 • 更新和更正了充分性决定的清单(7.5.2 节)。 • 提议的《隐私与电子通信条例》的有关现状。 • 少量的文字更正。 • “数据泄露”一词已被替换为 GDPR 中所使用的“个人数据泄露”。

目录

EXIN 隐私与数据保护基础

序言

本白皮书为参加 EXIN 隐私和数据保护基础（PDPF）考试的考生的备考文献。最新考试要求可参阅 EXIN 官方备考指南，具体可在 www.exin.com 下载。

在数字时代，有关人的信息变得越来越有价值。新技术的发展使组织能够大规模收集和存储数据。而当前的数据爆炸也带来了具体的安全挑战，特别是在因为欧盟关于个人数据保护的严格规定使得个人数据备受关注的当前。

对任何组织来说，隐私及个人数据的保护都必须是优先考虑的事务。

组织涉及处理居住在或正访问欧洲经济区（EEA）任一成员国的个人的数据时，都必须遵守《通用数据保护条例》（GDPR）。欧洲经济区以外的组织在欧洲开展业务时必须遵守该规定。遵守 GDPR 条例既避免罚款，同时增强用户信任。

拥有适当知识水平的专业认证人员，可以帮助组织准备和保持对 GDPR 的合规。EXIN 的隐私和数据保护培训项目涵盖了数据保护和 GDPR 合规所需的知识。

EXIN，2019 年 10 月

I. 隐私基础

1. 定义与历史背景

本章中我们将回顾隐私和数据保护的历史以及这两个概念之间的关系。在此基础上，我们将研究《通用数据保护条例》（GDPR）中的一些基本定义。部分术语和概念在 GDPR 第 4 条中有明确规定。GDPR 中使用的部分术语源于国际法。

1.1 数据保护条例的发展史

新近的发明与商业模式引起了对下一步需要加强个人保护、个人安全…“不被打扰”权…的注意。无数的机械装置使“壁橱中的窃窃私语将在屋顶大声宣布”这一预言成真。

来源：https://www.brandeis.edu/now/2013/july/privacy.html（截至 2017. 3.18）

可能有人认为这段话是最近写的，事实上路易斯·D·布兰代斯早在 1890 年《哈佛法律评论》的一篇文章中就写下了这些文字。用更现代的语言来说，这种不受打扰及侵犯的权利，最终成为 1948 年创立的《世界人权宣言》（UHDR）第 12 条的基础。

任何人的私隐、家庭、住宅或通信不得受到随意干扰，其荣誉及名誉也不容侵犯。人人都有权受法律保护免遭这种干扰或非难。

来源：https://www.un.org/en/universal-declaration-human-rights/（截至 2017.3.18）

20 世纪 70 年代，数据处理的快速发展，远程通信可能性的增长，恰巧与欧盟的发展所促进的跨境贸易相同步。由此，急需一套新的标准使个人能对其信息加以掌控。而与此同时，国际贸易则需要自由的国际信息流动。在保护个人自由的关切和支持整个欧洲自由贸易的可能性之间找到某种平衡就成为一个重要挑战。

欧盟成员国在《欧洲人权公约》（ECHR，1950）中签署了一项旨在整个欧盟维护人权的条约，其中包括尊重私人和家庭生活的权利。

1980 年，经济合作与发展组织（OECD）首次提出隐私保护和个人数据自由国际流动的相关法规：《隐私保护和个人数据跨国界流动指引》。这一指引在 1981 年借由《在自动处理个人数据方面的个人保护公约》正式确立，即《斯特拉斯堡条约》。

随着发展国际贸易和数据保护需求的日益增长，统一欧洲隐私法律的需求日益强烈。1995 年“数据保护指令 95/46 / EC”应运而生。

《欧盟基本权利宪章》（以下简称《宪章》，2002 年 12 月颁布）包含了《欧洲人权公约》规定的一般原则。《宪章》明确指出保护隐私和保护个人数据是一项基本权利：

第 7 条　尊重私人和家庭生活

1. 每个人的私人与家庭生活、居所和通信都有权受到尊重。

第 8 条　保护个人数据

1. 每个人的个人数据都有权受到保护。
2. 此类数据必须在特定用途和有关人员同意或法律规定的其他合法依据上进行适当处理。每个人都有权查阅已收集的有关其本人的数据，并有权对其进行纠正。
3. 对这些规则的遵守应受到独立机构的管控。

来源：　《欧盟基本权利宪章》。

尽管数据处理每年都在增长，但国际贸易仍受碍于不同的法规。尽管各成员国相关的法令与条例都源于 95/46/EC 号指令，但仍然存在着相当的差异。经过多年讨论，GDPR 于 2016 年 5 月 25 日颁布。GDPR 于 2018 年 5 月 25 日成为欧洲经济区各成员国法律。该条例废除了 95/46/EC 号指令。这意味着所有基于该指令的国内法将被 GDPR 所取代。

根据 GDPR 第 94(2)条，对已废除指令的有关引用，应被解释为对本条例的引用。针对根据第 95/46/EC 号指令第 29 条设立的个人数据处理保护的工作组的引用，应视为根据 GDPR 设立的欧洲数据保护委员会的引用。第 94 条明确指出，即使成员国需要更多时间来更新国内立法，以某种方式补充以 95/46/EC 指令为基础的法律，但不能混淆其所依何法。

1.1.1 数据保护历史概览

年份	名称	简称
1948	世界人权宣言	UHDR
1950	欧洲人权公约	ECHR
1981	关于个人数据自动处理的个人保护公约	ETS 108= 欧盟斯特拉斯堡条约
1995	保护个人在个人数据的处理及其自由流动方面权益的第 95 / 46 / EC 号指令	‘隐私指令’ （2018.5.25 后废除）
2002	欧盟基本权利宪章	‘欧盟宪章’
2016	通用数据保护条例(EU)2016 / 679	GDPR（2018.5.25 生效）
2016	2016/680 指令（刑事案件中的警务和司法合作）	
2016	2016/681 指令（关于乘客姓名记录（PNR）数据的使用）	

1.1.2 条例（Regulation） VS 指令（Directive）

与必须纳入每个成员国国内法的指令不同，条例具有约束力且直接适用于所有欧盟成员国。GDPR 是“与欧洲经济区（EEA）有关的文本”，这意味着它适用于所有欧洲经济区（EEA）国家，这些国家包括所有欧盟成员国，冰岛、列支敦士登和挪威。

1.2 GDPR 的适用范围与适用区域

1.2.1 适用范围

本条例适用于全部或部分以自动化方式处理的个人数据，以及非自动化处理方式下构成或预构成档案系统一部分的个人数据。

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 2(1)条

GDPR 适用于结构化的个人数据，包括从完全自动化的数据库系统到纸质文件，如某些医院仍使用的传统医疗档案。

存在一些例外：第 2016 / 680 号指令，而非 GDPR，作为国内法的依据，应用于共同外交和安全政策有关的活动，以及由主管当局为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚而进行的处理。

GDPR 也不适用于自然人**在纯粹个人或家庭活动过程中**处理个人数据。鉴于条款（18）将这些活动详细列为与专业或商业活动无关的活动，例如个人通信和为此目的保存的通讯录、或在此背景下开展的社交网络和相关的在线活动。

1.2.2 适用区域

1. 本条例适用于成立于欧盟内的个人数据控制者或处理者，无论处理工作是否在欧盟内进行。
2. 本条例适用于并非成立于欧盟，但处理欧盟数据主体个人数据的控制者或处理者，只要其数据处理活动涉及：
   a. 向欧盟的数据主体提供货品或服务，无论欧盟内的这些数据主体是否涉及支付；或
   b. 对其行为的监测是在欧盟内发生的。

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 3 条

不论数据处理在世界何处进行，在欧盟设立的控制者或处理者对个人数据进行的任何处理都应遵照 GDPR 执行。

GDPR 也适用于与贸易相关的处理（"提供商品或服务"）和"监测在欧盟人员的行为"（鉴于条款（23））。该规定影响深远。例如，一家加拿大公司正在处理一名阿根廷公民的个人网购数据。如果这名阿根廷公民碰巧在购买时正访问巴黎（法国），而且该加拿大公司知道它正在向欧盟提供商品或服务（因为他们将商品运往欧洲），则这一处理受到 GDPR 约束。

此外，GDPR 适用于不在欧洲经济区中成立，但在"成员国法律适用于国际公法的地方"处理个人数据的控制者。鉴于条款（25）给出了成员国的使馆或领事馆的例子。

GDPR 同样适用于在欧盟成员国注册的船舶，无论该船舶实际上在世界何地。

1.3 定义

在 GDPR 的最开始的几条鉴于条款中，对于隐私的定义就明确地与《欧盟基本权利宪章》相关联。

1. 自然人在处理个人数据方面受到保护是一项基本权利。《欧盟基本权利宪章》（简称《宪章》）的第 8(1)条和《欧盟运作条约》第 16(1)条规定，每个人的个人数据都有权受到保护。

2.关于保护自然人的原则及法令，在涉及到对其个人数据的处理时，无论其国籍或居住地，都应尊重其基本权利和自由，特别是保护个人数据的权利。

来源： 《通用数据保护条例》(EU) 2016 / 679; 鉴于条款(1)和(2)

据此，保护个人数据的权利是保护人的基本权利和自由的一种手段，其中包括人的隐私。

1.3.1 隐私

根据上述，隐私被定义为尊重一个人的私人和家庭生活、居所和通信的权利。

1.3.2 数据保护

综前所述，GDPR 是关于个人数据的保护，而非所有数据。GDPR 的第 4 条确明规定了哪些数据包括在其定义之内。

1.3.3 个人数据

GDPR 第 4(1)条将个人数据定义为：

“个人数据”是指与已识别或可识别的自然人（“数据主体”）有关的任何信息。可识别的自然人是指可以直接或间接查明的自然人，特别是参照如姓名、身份识别号码、位置数据、在线识别标识或该自然人的身体、生理、遗传、精神、经济、文化或社会身份的一个或多个具体因素;

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 4(1)条

任何信息都可以从字面上获取。它既可以是可被测度之物的“客观”信息，如血型、鞋子大小或血液中酒精含量。也可以是“主观”信息，例如关于一个人的看法（比如：“约翰是一个好教练”）。 “个人数据”不必是真实的或已被证明的。关于一个人的谎言或错误的数据仍然是“个人数据”。

“个人数据”的概念并不局限于那些可能被认为对个人私生活和家庭生活有害的信息。承载信息的的媒介也与此无关：个人数据的概念包括任何形式的可用信息：文本、图形、图像、摄影、视频、音频或任何其他可能的形式。

1.3.4 自然人

在法律上，“自然人”是指能够承担义务并拥有权利的人类。因此 GDPR 不适用于逝者（参阅鉴于条款（27））。欧盟成员国可规定有关处理逝者个人数据的规则。

1.3.5 直接、间接、假名化的个人数据

在实践中，我们区分三种类型的个人数据。

1. 3. 5. 1 直接个人数据

直接个人数据是无需额外信息就可以直接指向特定数据主体的数据。例如，数据主体的照片、DNA、指纹。如果姓名非常特殊，那么它可以是直接的个人数据。大多数姓名并不唯一，通常是非直接的个人数据。一个独特的头衔，如“现任法国总理”，也是判定一个人的直接参考，即直接的个人数据。

1. 3. 5. 2 间接个人数据

间接个人数据是可以或可能在将来使用附加信息关联到特定数据主体的数据。例如，汽车的车牌是间接的个人数据，因为有可能使用附加信息跟踪到汽车的所有者（该情况下，数据库中的信息是与汽车所有者有关的车牌号）。对于由政府分配给个人的唯一号码（社会保障号码）或由 ISP 分配给人人们的唯一号码（IP 地址）也如此。事实上，并非每个控制者都能够追踪到相关个人的车牌、社会保障号码或 IP 地址，但这并不重要。理论上可识别到个人就使得它成为（间接的）个人数据。

如果是常见的且不指向特定的人，姓名就是间接个人数据。用“詹姆士·威廉姆斯”这个名字来区分本人和其他人，就需要更多的信息，如住所和生日。

1.3.5.3 假名化的个人数据

数据假名化是掩盖身份的过程。该过程的目的是能够收集关于一个人的额外数据而无需知道其身份。一个可能的例子是用摄像头记录桥梁道路上通行汽车的数量。车牌号码是（间接）个人数据。控制者将使用唯一密钥或假名替换每个车牌号码，保存一个独立的表，连接每个密钥到相应车牌。控制者可能随后将假名化数据传送给处理者，而将秘钥保存在一个安全的地方。

假名化数据是一种间接的个人数据，其中识别数据主体（“密钥”）所需的附加数据仅对控制者可用。只要密钥存在，该过程是可逆的，因此关于人的假名化数据仍被认为是个人数据，因为身份识别在技术上仍是可能的。

而匿名化意味着数据所涉及的任何人都不能以任何方式所识别。匿名数据**不再**被认为是个人数据。而假名化数据能够通过销毁秘钥而实现匿名化。

例如：对于一个健康和饮食习惯的市场调查，一组选定的受访者接受电话访谈。应答者的姓名、电话号码和其他数据是已知的并保存在数据库中，数据对象对此给予了许可。这些数据主体在研究过程中被拨打了多次。一旦研究完成，在收集了所需要的信息后，所有的可识别身份的数据会被删除。这意味着这些数据不能指向到到特定的数据主体。只有像男性/女性和年龄段的信息会被关联到有关健康和饮食习惯的数据。换句话说，在研究之后留下的数据是匿名的。

1.3.5.4 特殊个人数据

GDPR 区分了一些值得特别关注的个人数据类别。 特殊个人数据类别包括：

- ✓ 揭示种族或民族血统的数据
- ✓ 揭示政治观点的数据
- ✓ 揭示宗教或哲学信仰的数据
- ✓ 揭示工会会员身份的数据
- ✓ 基因数据
- ✓ 为唯一识别自然人而处理的生物特征数据
- ✓ 关于健康的数据
- ✓ 关于自然人性生活或性取向的数据

除 GDPR 第 9 条中明确提及的情况外，禁止处理特殊的个人数据。

1.3.6 处理

GDPR 所指的处理数据一般指个人数据的处理。GDPR 不适用于任何其他数据的处理。即使这样，GDPR 对数据处理的定义仍非常宽泛：

“处理”指对个人数据或个人数据集执行的任何单一或组合操作，如收集、记录、组织、结构化、存储、更改、检索、咨询、使用、传输、传播或以其他方式提供、排列或组合、限制、删除或破坏数据，无论是否通过自动化手段

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 4(1)条

事实上，很难想象有不被包含在该定义之中的个人数据的处理方式。

收集个人数据、存储个人数据、销毁个人数据都属于处理，即使是对不属于你的一个服务器进行备份，只要其包含个人数据，也将被视为一种存储，而这也包含在该定义中。

1.4 角色、责任、利益相关者

1.4.1 控制者

“控制者”指单独或共同决定个人数据处理目的和方法的自然人、法人、公共当局、机关或其他机构。

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 4(7)条

控制者是**负责确定处理目的和手段**的自然人或法人。

1. 考虑到数据处理的性质、范围、背景和目的，以及对自然人权利及自由产生危害的可能性，控制者应实施适当的技术和组织措施以确保并证明该处理是按照本条例进行的。这些措施应在必要时加以审查和更新。
2. 当与处理活动相称的情况下，第 1 条所指的相应措施应包括由控制者实施适当的数据保护措施。

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 24 条

换言之，控制者的责任和作用是执行适当的技术和组织措施以遵守 GDPR，其中包括“适当的数据保护政策”。

第 24.1 条表明，所需的技术措施水平可以根据具体情况和所涉自然人的风险程度而有所不同。

例如，虽然同为个人数据的处理，曲棍球俱乐部的夏季烧烤邀请与一组慢性疾病患者的邀请可能需要不同级别的数据安全性。参见 1.3.5.4：特殊个人数据。

需要注意的是，控制者的角色不只是适当程序的技术实施。控制者应对处理过程的 GDPR 合规负责，并且必须能够提供证明。

1.4.2 处理者

“处理者”指代表控制者处理个人数据的自然人、法人、公共当局、机关或其他机构

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 4(8)条

处理者通常指“数据处理者”， 该定义表明处理者总是“代表控制者”而行动且必须遵从控制者的指令。这些指令应被写入合同中。控制者-处理者合同在第 8.2 章：“控制者与处理者书面合同”中有讨论。

1.4.3 数据保护官（DPO）

控制者和处理者可以，且在下面列举的情况下**必须**任命一名数据保护官（DPO）。DPO 的的正式责任是确保该组织了解并遵守 GDPR 及成员国法律要求的数据保护义务和责任。

在如下情况，控制者和处理者应指定一名数据保护官：

（a）处理工作由公共机关或机构进行，基于其司法职能行事的法院除外。

（b）控制者或处理者的核心活动包含的处理工作，由于其性质、范围和/或目的，需要定期和系统地大规模监测数据主体，或者

（c）控制者或处理者的核心活动涉及第 9 条所述大量特殊类别的数据及第 10 条所述与刑事定罪和犯罪有关的个人数据

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 37(1)条

非必须指定 DPO 的组织，可自行决定是否任命 DPO。如果一个组织自愿任命一名 DPO，该 DPO 应遵守 GDPR 的标准。一旦 DPO 被任命，组织必须通知有关监管机构并公布 DPO 的详细信息，以确保数据主体可联络。根据鉴于条款（97） ，数据保护官应是“具有数据保护法律和实践专业知识的人员”。

GDPR 第 38 条明确要求控制者和处理者确保数据保护官适当和及时地参与与保护个人数据有关的所有问题。控制者和处理者有义务支持 DPO 开展工作，提供必要资源来使 DPO 开展这些工作、接触涉及的个人数据及其处理操作，并保持其专业性。DPO 具有**独立立场**并受到 GDPR 的保护：

控制者和处理者应确保数据保护官不会收到有关执行这些任务的任何指令。数据保护官不得因执行其任务而被控制者或处理者解雇或处罚。数据保护官应直接向控制者或处理者的最高管理层汇报。

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 38(3)条

1.4.3.1 DPO 的职责

数据保护官的职责至少包括以下内容：

（a）向控制者或处理者，以及依据本条例和依据其他联盟或成员国的数据保护规定来履行其义务的雇员提供咨询及建议;

（b）监测对本条例、其他联盟或成员国的数据保护规定、以及控制者或处理者在保护个人数据方面的政策的遵守情况，包括职责分配、认识提高和对参与处理业务的工作人员培训，以及相关审计;

（c）根据要求，就数据保护影响评估提供咨询意见，并根据第 35 条监督其执行情况;

（d）与监管机构合作;

（e）就数据处理有关的事务（包括第 36 条所指的事先协商），担任监管机构的联络人，并酌情就任何其他事项进行协商。

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 39(1)条

1.4.4 接收者

“接收者”是指向其披露个人数据的自然人、法人、公共当局、机关或其他机构，无论其是否为第三方。但是，根据欧盟或成员国法律要求接收特定结构化调查数据的公共当局，不应被视为接收者；公共当局对这些数据的处理应按照处理的用途，遵守相应的数据保护要求。

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 4(9)条

该定义主要告诉我们谁**不是**接收者。接收者是披露的个人数据和/或个人数据处理结果的重要利益相关者。特别是，当接收者是在欧洲经济区之外，尤其是当接收者是欧洲经济区以外的一个政府机构，则有着更严格的规定，这些规则将在后续讨论。见 7.4： 跨境数据传输。

1.4.5 第三方

“第三方”是自然人或法人，公共当局，机构或实体，但数据主体、控制者、处理者以及在控制者或处理者直接授权下处理个人数据的主体除外；

来源： 《通用数据保护条例》(EU) 2016 / 679; 第 4(10)条

第三方是“自然人，要么是法人、公共当局、机构或团体”。无论如何，不是数据主体、控制者、处理者，也不是“在控制者或处理者的直接授权下处理个人数据的人”。那什么是第三方？

原则上，第三方是无合法依据或没有得到授权来处理个人数据的个人或组织。一个例子是会计师，他在履职时可能无意中看到个人数据。或者系统管理员，他在检查个人数据备份是否成功时，碰巧看到一些姓名和其他个人数据。

接收个人数据的第三方——无论是合法的还是非法的——都被视为处理个人数据。当处理不是在控制者的直接授权下执行的，那么“第三方”原则上将被视为新的控制者。

2. 处理个人数据

根据关于处理的的定义，任何涉及个人数据的操作都包含在处理的定义中。 GDPR 第二章（第 5 至第 11 条）详细规定了数据处理的原则。

2.1 数据处理原则

处理个人数据时，必须遵守处理个人数据的原则。 这些原则是：

- 合法、公平与透明
- 目的限制
- 数据最小化
- 准确
- 留存限制
- 完整和保密
- 可问责

2.1.1 合法、公平和透明

对数据主体的个人数据应以合法、公正和透明的方式处理。数据主体如果还不清楚其数据如何被处理，可以提出问询。

2.1.2 目的限制

收集个人数据的目的应具体、明确和合法，**不得**以与初始目的不符的方式做进一步处理。

可做进一步处理的情况：

- 涉及公共利益的存档
- 科学或历史研究
- 统计目的

前提是应符合 GDPR ，同时能够为数据主体的权利和自由提供适当的保障措施。

2.1.3 数据最小化

个人数据处理应确保充分、相关和**仅限于**与处理目的有关的**必要信息**。

2.1.4 准确

个人数据应当准确，必要时应及时更新：应采取一切合理步骤确保不准确的个人数据得到纠正或删除。

2.1.5 留存限制

对能识别数据主体的个人数据的留存，不得超过特定用途下处理个人数据的所需要的时长。

2.1.6 完整和保密

个人数据的处理方式应确保个人数据的适当的安全性，包括利用适当的技术或组织措施防止未经授权的或非法的处理，避免意外的丢失、破坏或损坏。

2.1.7 可问责

控制者为数据的处理承担责任。 这表明控制者和处理者都有责任确保上述原则的遵守。控制者还必须能够证明其遵守了这些数据处理的原则。

3. 合法依据与目的限制

3.1 处理的合法依据

根据 GDPR 第 6.1 条，只有在适用以下**至少一条**的情形下，处理数据才被视为合法。

- ✓ 数据主体同意基于一个或多个特定用途对其个人数据进行处理。
- ✓ 处理是为履行数据主体为当事方的合同，或在签订合同前所必需的：合同签订前的数据处理，只要是基于数据主体在签订合同前的请求来采取的步骤，即是合法的。
- ✓ 处理是控制者为了履行其法律义务所必需的。
- ✓ 处理是保护数据主体或另一个自然人的切身利益所必需的。
- ✓ 处理是执行公共利益领域的任务或行使控制者既定的公务职权所必需的。
- ✓ 处理是实现控制者或第三方的合法利益所必需的。
  - ■ 除非：要求保护其个人数据的数据主体的基本权利和自由高于此利益，尤其是数据主体为儿童的情况下。

此合法依据的清单是详尽无遗的。在 GDPR 下关于处理个人数据没有其他合法依据。

3.1.1 目的限制和用途说明

目的限制作为一个术语，在 GDPR 中没有明确的定义。 但是在 2013 年 4 月，由欧洲监管机构，欧洲数据保护主管和欧盟委员会代表组成的第 29 条工作组（WP29）发布了关于处理个人数据的目的限制原则的意见。WP29 的意见为欧盟数据保护规则提供了官方性的指导。

从 2018 年 5 月起，第 29 条工作组由 GDPR 第 68 条所定义设立的欧洲数据保护委员会（EDPB）所接替。在其第一次会议上，EDPB 确认了由 WP29 发布的关于 GDPR 和其他文件，以确保连续性。2018 年 5 月之前发布的许多指导方针和意见都被整合或引用到 GDPR 中。

个人数据必须针对特定用途而收集。因此，控制者必须认真考虑将个人数据用于何种用途，且不得收集对于该用途不必要、不胜任、不相关的个人数据。

来源：WP29 关于目的限制的意见，III. 1.1（用途必须明确）（截至 2019.7.24）

GDPR 第 5(1)(b)条规定，“个人数据的收集必须基于特定、明确和合法的目的(…)”。让我们看看这句话的要点：

3.1.1.1 明确

为了确定数据处理是否符合法律并采用哪些数据保护保障，确定收集个人数据的用途是一个必要的先决条件。因此，目的明确化对控制者使用所收集的个人数据的目的设置了限制，并有助于建立必要的数据保护保障措施。

用途的明确化要求由数据控制者进行内部评估，这是保证其可问责性的必要条件。控制者应遵循这一关键步骤，以确保遵守适用的数据保护法律。控制者必须确定用途是什么，且必须记录并能够证明已经执行了这种内部评估。

来源： WP29 关于目的限制的意见（截至 2019.6.24）

因为收集个人数据即处理个人数据，在收集个人数据之前就必须明确其用途。

需要明确的用途必须足够详细，以确定哪些类型的处理包含在指定用途中，哪些类型的处理不包含在指定用途中。 含糊或笼统的用途，例如"提高用户体验"、"营销用途"或"未来研究"——如果没有更多细节——通常不符合"明确"的标准。向数据主体发送“处理浏览信息以呈现与他们兴趣相关的广告”的信息，将准确地说明用途是什么以及如何实现。

3.1.1.2 清晰

收集个人数据必须基于清晰的用途。收集的用途不仅必须在负责收集数据的人的脑中是明确的，它们还必须清晰地表达出来。 换言之，必须以某种可理解的形式清楚地揭示、解释或阐述其用途。由此前的分析可以推断，这项要求应不迟于开始收集个人数据时完成。

这项要求的最终目标是确保用途清晰，没有意义模糊或歧义。内涵必须清晰、无疑义、容易理解。尤其是，用途的清晰化必须以适当的方式进行表达，以保证控制者（包括所有相关人员）和任何第三方处理者，以及数据保护机构和相关数据主体都能对它有相同的理解。应特别注意确保对任一用途的说明对于来自不同文化或语言背景、具有不同理解程度或特殊需求的所有相关方都足够清楚。

来源： WP29 关于目的限制的意见（截至 2019.7.24）

清晰的用途说明，能使控制者打算如何使用收集到的个人数据变得透明。它能帮助所有代表控制者处理数据的人，以及数据主体、监管机构和其他利益相关方对如何使用数据有一个共同理解。相应的，这也降低了数据主体与控制者二者期望不同的风险。

3.1.1.3 合法

合法性的要求意味着数据处理的用途必须在最广泛的意义上“合法”（GDPR 第 6.3 条）。这包括所有形式的成文法和普通法、初级和次级立法、市政法令、司法判例、宪法原则、基本权利、其他法律原则以及法学知识，这类“法律”将会为主管法院所解释和考量。

在其他的法律规定之外，GDPR 的 6(1)条始终适用于个人数据的处理。为了使处理合法，数据处理必须在任何时候都基于六大合法依据中的至少一项。（参加见 3.1 合法依据）。

3.1.2 相称性和辅助性

3. 根据辅助性原则，在不属于欧盟专有权限的地区，除非成员国在中央一级或区域和地方一级无法充分实现拟议行动的目标，且由于拟议行动的规模或影响，在欧盟一级能够更好地实现这些目标的情况下，欧盟才应采取行动。 （...）
4. 根据相称性原则，欧盟行动的内容和形式不得超过实现条约目标所必需的范围。

来源：《欧盟运作条约》第 5 条

这似乎与保护隐私和个人数据的实践关系甚远，但事实并非如此。 这些原则构成了整个 GDPR 的一条红线，直至实操层面。

3.1.2.1 辅助性

除本条约外，辅助性还体现在要求只有当**没有其他手段能够实现目的**的情况下才能处理个人数据的通用规则中。处理的六项合法依据中的五个都要求处理应是绝对必要的。当有其他的方法来达成目的，就很难声称处理个人数据是必要的。

举例来说，如果一个人想要弄清楚通常周六下午有多少人走在购物街上，出于该目的，你并不需要区分个体。可以通过利用智能手机的手机信号（例如其 MAC 地址）来统计人数。然而，由于 MAC 地址能够追踪到持有智能手机的个人，这也被认为是个人数据。一定有其他方法能够在不使用个人数据的情况下计算出人数。你可以通过例如设置观察员来简单统计人数。依据 GDPR 中的辅助性原则，使用 MAC 地址信号就是非法使用个人数据，因为你统计顾客数的利益逾越了这些顾客的基本隐私权益。你将不得不使用一种保持顾客匿名且不收集直接或间接的个人数据的方法。

3.1.2.2 相称性

相称性原则与辅助性密切相关。相称性要求欧盟采取的任何行动不应超出实现条约目标所必需的范围。当应用于个人数据处理时，这意味着超出其必需的数据不应该收集。我

们认为，这在操作层面上符合数据最小化原则：“个人数据应该是够用的、相关的，仅限于与其处理目的有关的必要数据”。 这点似乎显而易见，但我们都知道很多收集的数据超出了其目的所需的例子。例如，当一家网络商店在送货地址表格中收集性别数据时，这对于将产品发送给客户来说是不必要的。

4. 数据主体的权利

从隐私和数据保护的历史来看，我们认为数据主体的基本权利是至关重要的。GDPR 规定，除非符合若干要求，否则禁止处理个人数据。 这类处理必须有一个合法的理由。处理的目的必须明确规定。除此之外，如果还有除了处理个人数据之外的其他方法来达到其特定目的，那么就应采用这些其他方法。

即使在满足所有要求的情况下，控制者也必须在任何时候在数据主体的基本权利和处理的目的间取得平衡。毫无疑问，GDPR 的大量篇幅是专门针对数据主体的权利的。

4.1 透明的信息、沟通与形式

GDPR 的一个基本观点是，无论何时，数据主体在其个人数据被处理时都必须被告知。如果处理是基于同意的，数据主体应该知道和理解其同意的是什么（“知情同意”）。

当处理是基于一个或多个其他合法处理依据，数据主体仍应被告知其哪些个人数据将要或正在被处理、以及起处理目的和责任人。通过“知晓”和“被告知”，GDPR 明确要求“知悉”和“充分理解”。

控制者应当采取适当措施，向数据主体提供本条例第13条和第14条涉及的任何信息，与数据主体做本条例第15条至第22条和第34条要求下的有关数据处理的沟通，尤其是需要提供给儿童的任何信息。该种信息应当以一种准确、透明、易于理解、易于获取的方式提供，且应使用清楚、平实的语言。该种信息应以书面或者其他适当方式（如电子方式）提供。在应数据主体的要求且数据主体的身份已通过其他方式加以证实的情形下，该等信息可以以口头形式提供。

来源：《通用数据保护条例》(EU) 2016 / 679；第 12(1)条

以下各段将讨论上述条款并详细描述数据主体在处理个人数据时所拥有的各种权利。

控制者应当为数据主体行使其在本条例第15条到第22条项下的权利提供便利。在本条例第11条第2款规定的情形下，控制者不应拒绝数据主体行使其在本条例第15条到第22条项下的权利的要求，除非控制者能证明其无法识别数据主体。

来源： 《通用数据保护条例》(EU) 2016 / 679; 第12(2)条

响应数据主体的诉求有两个重要的例外。

- 首先，控制者可能（而且常常必须）要求数据主体提供身份证明。 这有助于降低第三方非法获取个人数据的风险。

- 第二，如果无法识别其处理的哪些数据与有关数据主体相关，则控制者可免除其遵从数据主体特定权利的义务。

第 12 条第 2 款至少同样重要。享有这些权利固然很好，但是当某些公司或政府机构告诉人们他们的数据在被有目的地处理时，并不是每个人都有足够的能力行使其权利。

根据第 12 条第 2 款，控制者在计划处理数据时就必须通知数据主体他们所拥有的权利，并协助他们行使这些权利。所要进行的数据处理的相关信息，以及对数据主体的帮助，都应免费提供。如果无视这一义务，控制者可能会面临巨额的罚款（参见 7.3.3）。

4.2 有关个人数据的信息及个人数据查阅

除第1段提到的信息之外，控制者在获取个人数据时，出于证明处理过程公正和透明的需要，在必要的情况下，还应当向数据主体提供以下进一步的信息：

来源：《通用数据保护条例》(EU) 2016 / 679; 第13(2)条

4.2.1 任何情况都应提供给数据主体的信息

对于要处理的个人数据是从数据主体（GDPR 第 13 条）处收集还是从其他来源（GDPR 第 14 条）收集的不同情况，在必须向数据主体提供哪些信息上存在细微差别。

在所有情况下，控制者必须提供：

✓ 控制者及其代表的身份和联系方式（适用的情况下）
✓ 数据保护官的详细联系方式（适用的情况下）
✓ 个人数据处理的目的
✓ 处理的法律依据

此外，如果处理的合法依据是“控制者或第三方追求的合法利益”时：

✓ 个人数据的接收者或者接收者的类别（如果存在）；

4.2.2 当传输个人数据时须提供给数据主体的信息

如果控制者打算将个人数据传输到第三国或第三国际组织，则应提供更多的细节。

✓ 个人数据存储的期限
✓ 数据主体享有的
  - 要求从控制者处查阅自身个人数据的权力
  - 要求纠正、删除个人数据的权力

- 要求对数据处理活动进行限制的权利
- 反对对其个人数据进行处理以及要求数据可携带的权利

✓ 如果数据处理是基于同意进行的，则数据主体可以随时撤回其之前作出的同意，但是该撤回不影响撤回之前，根据数据主体同意所对数据进行处理的合法性；
✓ 向监管机构提起申诉的权利；

4.2.3 当个人数据并非从数据主体处直接获取时须额外提供的信息

当个人信息并非从数据主体处获取时，需要提供一些额外的信息：

✓ 涉及个人数据的类别
✓ 个人数据接收者或接收者的类别（如果存在）
✓ 个人数据的来源，以及是否来源于公开渠道（适用的情况下）

4.2.4 提供相关信息的时机

控制者应在以下情况下提供上述资料：

✓ 应在获取个人数据之后的合理期限内，最迟不超过一个月；
✓ 数据处理时涉及的特定情况；
✓ 如果个人数据将要用于与数据主体的通信，则最迟应该在与数据主体第一次通信之前提供；
✓ 如果已经预见到个人数据将要披露给其他数据接收方，则最迟应该在个人数据首次披露之前提供；

对于特殊情况，有一些额外的义务，也存在对上述规则的一些例外。参见 GDPR 第 15.4 条。

4.3 数据主体的查阅（检查）权

数据主体应当有权从控制者处确认与其相关的个人数据是否正在被处理，并在确认控制者正在对其个人数据进行处理的情况下，有权要求查阅与其相关的个人数据（…）

来源： 《通用数据保护条例》(EU)2016 / 679; 第15(1)条。

尽管有上述关于被告知的规则，但数据主体在任何时候都有权从控制者处获得其个人数据是否正在处理的有关信息。

如果数据正在被处理，控制者有义务提供上述信息和一个正在处理的免费数据副本。数据的额外副本可以向数据主体收取费用，但只能依据管理费用收取合理价格的费用。

对于数据主体获取其已被处理或待处理的个人数据副本的权利，有一项重要限制：该请求不得对他人的权利和自由产生不利影响。

4.4 纠正与删除

4.4.1 纠正权

当数据主体从控制者那里获取关于他或她的个人数据副本时，数据主体可能会发现数据是错误的。这种情况下，数据主体可要求纠正：

数据主体有权要求控制者对其不准确的个人数据进行及时纠正。考虑到处理的目的，数据主体应当有权要求控制者完整化其个人数据，包括通过提供补充声明的方式。

来源： 《通用数据保护条例》(EU)2016 / 679; 第16条。

4.4.2 删除权（被遗忘权）

在某些情况下，数据主体有权删除他们的数据。这种情况通常是在处理过程不能满足 GDPR 的要求时。可以对控制者行使该权利，他们必须作出回应，且不得无故拖延（尽管在困难情况下可以延期，但必须在一个月内）。

数据主体有权要求控制者对其个人数据进行删除，并且控制者有义务及时地删除个人数据，不得无故拖延（…）

来源： 《通用数据保护条例》(EU)2016 / 679; 第17条。

删除个人数据的理由可以是：

- ✓ 就获取或处理的目的而言，该个人数据已非必要
- ✓ 撤回之前的同意
- ✓ 收集数据是为了直接向 16 岁以下儿童提供信息服务
- ✓ 反对其处理 （参见下文）
- ✓ 非法处理
- ✓ 为遵守欧盟或控制者所属成员国法律规定的法定义务

基于这些理由的删除权，只有在某些理由是处理的唯一合法理由时才有效。举例来说，数据主体因不再予以同意而要求政府删除计算其所得税所需的个人数据将不会被支持，因为在这种情况下，“同意”不是其合法处理的依据。

4.4.3 限制处理的权利

在某些情况下，数据主体应当有权限制控制者处理其数据。限制处理的理由可以是：

- ✓ 数据主体对数据的准确性提出质疑；
  - ■ 在核实申请和更正数据所需的时间内，对个人数据的处理进行限制；
- ✓ 处理是非法的，但是数据主体反对删除该个人数据，而是要求限制使用该个人数据；
- ✓ 出于其处理目的，控制者不再需要该个人数据，但数据主体为提出、行使或抗辩法律诉求而需要该个人数据；
- ✓ 在等待核实控制者的法律依据是否优先于数据主体的法律依据前，数据主体已按照21条第1款（反对权）反对控制者对其个人数据进行处理

当处理过程被限制时，意味着什么？

如果处理行为在第1款中受到限制，除存储之外，这些个人数据只应在数据主体同意，或为提起、行使或抗辩法律诉求、为保护其他自然人或法人的权利，或为了欧盟及成员国重要公共利益的情况下才能被处理。

来源： 《通用数据保护条例》(EU)2016 / 679; 第18(2)条。

控制者必须在解除限制之前通知数据主体。

4.4.4 通知责任（纠正/删除/限制处理）

除非被证明不可能完成或者需要不成比例的工作量，控制者应当将根据第16条、第17条第1款以及第18条，对个人数据进行的任何纠正、删除或者处理限制告知个人数据的接收者。如果数据主体要求，控制者应当向数据主体告知上述数据接收者。

来源： 《通用数据保护条例》(EU)2016 / 679; 第19条。

该责任意味着，除了实施确保数据主体的权利的系统和程序外，控制者必须实施相关的系统和程序，向受影响的第三方通知对这些权利的行使。

Cartoon © Pierre Kroll, derived with authorization from the leaflet 'Take Control of your Personal Data' (2012), ISBN 978-92-79-22654-0, Published by European Commission - Directorate-General for Justice

4.4.5 数据可携权

数据主体有权以结构化的、通用的、可以机读的方式接收其提供给控制者的与其相关的个人数据，并且有权将这些数据传输至其他控制者，而不受此前已经获得这些数据的控制者的妨碍。（…）

来源： 《通用数据保护条例》（EU）2016 / 679; 第20条。

如果处理是基于知情同意或合同进行的，**并且**处理是通过自动化手段进行的，数据主体有权接收其个人数据或将其个人数据在控制者之间传输。数据主体有权将账户明细从一个在线平台迁移到另一个平台。

这项权利将使客户更容易更换到其他在线服务商，例如网上商店或其他在线业务。设立一个新账户应变得更容易，控制者必须允许账户信息传输给竞争对手。

请注意，数据可携权**不适用**于为了公共利益，或在控制者行使被赋予的官方权力时所必需的处理。

4.5 反对权和自动化的个体决策

4.5.1 反对权

正如 3.1 节“处理的合法理由”所述，控制者必须有处理个人数据的合法依据。，然而即使合法依据是“公共利益”或“正当利益”（包括剖析——有时也称用户画像或用户测写），数据主体仍可有权反对这种处理。

GDPR 要求组织证明，要么有令人信服的理由继续处理，要么就其法律权利而言这种处理是必须的。如果不能提供这两个理由之一的证明，就必须停止相应的处理活动。

4.5.2 自动化的个体决策，包括剖析

为直接营销目的对个人数据进行处理（无论是首次处理或再处理）的，数据主体应有权随时反对该等数据处理（包括与该类直接营销有关的剖析活动），且无需就此承担任何费用。控制者应明确告知数据主体享有该等反对权，并且对该等反对权的告知应与其他信息分开呈现给数据主体。

来源： 《通用数据保护条例》（EU）2016 / 679; 鉴于条款第70条。

数据主体有权反对出于直接营销为目的个人数据处理，包括剖析。

第 22.1 条还规定，数据主体有权不受纯粹基于自动处理决策的约束。但是，如果决策是基于数据主体的明确且知情同意做出的，则本条不适用。

4.6 向监管机构提出申诉的权利

在不影响任何其他行政或司法救济的情况下，如数据主体认为对其个人数据的处理违反本条例，则有权向监管机构申诉，特别是向其经常居住地、工作地或涉嫌违法行为地所在成员国的监管机构申诉。

来源： 《通用数据保护条例》（EU）2016 / 679; 第77(1)条。

数据主体有权就其个人数据的处理向其所在成员国，或在侵害行为发生地的成员国监管机构提出申诉。GDPR 包含一些规则，以确保所有当事方，包括涉及的单个或多个控制者、处理者和监管机构，维护数据主体获得有效司法救济的权利。

5. 个人数据泄漏及相关程序

5.1 个人数据泄漏的概念

“个人数据泄漏”是指违反安全规定对个人数据进行传输、储存或其他方式的处理，导致个人数据意外或非法破坏、丢失、篡改、未经授权披露或查阅；

来源： 《通用数据保护条例》(EU)2016 / 679; 第15(1)条。

根据 GDPR，每次数据泄露**都是**一个安全事件。 它不仅仅是一个漏洞缺陷（安全风险）或安全威胁，而是安全经理的噩梦变为现实且有人已经接触了数据。

对于一次个人数据泄露，该安全事件必然导致个人数据已经或可能被非法处理的局面。而这也意味着，并不是所有的安全事件都是数据泄露。记住，破坏、储存和复制也被认为是处理过程。

有关“数据泄露”的条款里经常例举的场景包括恶意或善意的黑客入侵和“第三方”未经授权访问个人数据等。但 GDPR 中关于个人数据泄露的定义要广义得多。

数据中心的火灾很可能会严重损毁存储在那里的个人数据。这既是安全事件，因为数据不再可用，又是一次个人数据泄露，因为数据已未被授权地处理，本例中为损毁。

类似的，当处理者意外地删除了个人数据，处理者违反了 GDPR 第 29 条，而使处理成为非法。

处理者以及任何在控制者或处理者授权下活动且能接触个人数据的人员，如没有控制者的指示，均不能擅自处理这些数据，除非有欧盟或成员国法律要求。

来源： 《通用数据保护条例》（EU）2016 / 679; 第29条。

在该条例中，“数据泄露”这个术语经常用于指“个人数据泄露”。不同之处在于，根据上下文的不同， “数据泄露”也可以指商业的或其他的类型的公司数据被泄露的情况。个人数据泄露也属于数据泄露。涉及个人数据的数据泄露，就是个人数据泄露。

5.2 个人数据泄漏发生时的处置程序

GDPR 第 32 条要求控制者和处理者“执行适当的技术和组织措施，以确保安全等级能够与风险相应”。

有一些国际认可的信息安全标准，如 ISO/IEC27001，这些标准提供了用于修复损害并防止事件再次发生的事故处理程序。

个人数据发生泄露，若不及时妥善处理，可能会对自然人产生人身的、物质性或非物质性的损害，例如丧失对其个人数据的控制或者使其自由或权利受到限制、歧视、身份盗用或诈骗、财务损失、未经授权的假名化移除，名誉损害、具有职业保密性的个人数据被公开或任何其他重大的经济或社会不利影响。

来源： 《通用数据保护条例》(EU)2016 / 679; 鉴于条款（85）。

5.2.1 向监管机构通知个人数据泄漏

当发生个人数据泄露，数据控制者必须通知**监管机构**。控制者一旦知悉个人数据发生泄露，应当及时（可行时应不得迟于意识到泄露后的72 个小时）通知监管机构，不得无故拖延。

如在发现个人数据泄露后的 72 小时后才通报有关个人数据泄露，则必须在通知书内提供延误的充分理由。

第33.1条规定了对数据泄露通知要求的一个重要例外：如果“个人数据泄露不大可能对自然人的权利和自由造成风险”，则不需要通知。

5.2.2 向控制者通知个人数据泄露

当数据处理者遭遇了个人数据泄露时，他们必须在发现个人数据泄露后立即通知**控制者**，不得无故拖延。

根据 GDPR，处理者没有其他通知或报告义务。所有通知和通告必须由控制者来完成。

5.2.3 向数据主体通知个人数据泄露

如果控制者认定个人数据泄露“可能会对个人的权利和自由造成高风险”，他们必须向受影响的**数据主体**通知有关其个人数据泄露的信息。根据第 34 条，这是必须执行的，且“不得无故拖延”。

通知数据主体的附加要求中有三个例外，以下情况下通知数据主体**不是**强制的：

- ✓ 当数据不可读
- ✓ 当采取了其他最小化风险的措施
- ✓ 当通知需要不相称的努力

5.2.3.1 加密与其他保护措施

控制者“实施了适当的技术和组织保护措施”，这些措施“使未经授权访问数据的任何人无法理解数据，例如加密”。

5.2.3.2 缓解措施

控制者在发生个人数据泄露之后采取相应行动，以“确保数据主体的权利和自由面临高风险”不太可能出现。

5.2.3.3 不相称努力

当通知每一个数据主体需要不成比例的努力，这种情况下，可采用替代的通信措施，例如在公司网站上通告。

5.3 个人数据泄漏的类别

可将个人数据泄露分为三类，它们分别是：

- ✓ **不太可能**对自然人的权利和自由造成风险的数据泄露；
  - 不强制通知数据泄露
- ✓ **可能会**对自然人造成的人身的、物质或非物质损害的数据泄露
  - 必须通知监管机构
- ✓ **可能会**对个人的权利和自由造成高风险的数据泄露
  - 必须通知监管机构
  - 必须通知数据主体（如果可行）

数据保护的组织化

6. 数据保护对组织的的重要性

几乎所有的组织都处理个人数据。对于一个处理个人数据的组织，数据保护不仅仅是一项法律要求或避免处罚的手段，它也维系到组织的声誉。

专业地处理个人数据意味着对数据的质量保障、安全管理与治理。

以下各段将概述合法处理个人数据的有关要求。

6.1 GDPR 的合规要求

GDPR 中规定，除非满足 GDPR 的相关要求，否则禁止任何组织处理个人数据。以下为必须满足的要求。

6.1.1 符合个人数据处理的原则

特别是，2.1 节中所规定的数据保护原则必须满足。其目的必须清楚、详细和具体，而且必须适用六项可能的"法律依据"中的至少一项。 必须保障数据主体的权利，且必须有充分的保护措施。

6.1.2 法律责任框架

GDPR 要求控制者、处理者以及任何一个处理个人数据的个人都应当遵守 GDPR。控制者作为确定数据处理目的和手段的一方，有义务执行适当的技术和组织措施，以确保按照 GDPR 进行处理。

正如我们在 1.4.1 节中看到的那样，控制者还应对处理者所执行的这些"适当措施"负责，以确保处理工作符合条例规定的数据处理原则（另见 2.1 节）。 因此，除非事先获得来自控制者具体或通用性的书面授权，处理者不能将部分处理外包给一个子处理者。

处理者只应根据控制者的文档指令来处理个人数据。必须订立一份对处理者具有约束力的法律合同。它将处理者受约束于控制者并规定：

- ✓ 处理的主题
- ✓ 处理时长
- ✓ 由控制者定立的处理性质和目的

✓ 涉及个人数据的类型
✓ 数据主体类别
✓ 控制者的义务和权利。

为了**证明符合**这些要求，控制者和处理者需要记录它们是如何符合的。其中一些记录是强制性的，并且具有规定的格式。当出现问题或监管机构有其他理由检查合规的情况时，还需要其他文档。

6.1.3 影响评估

当特别是使用了新技术进行处理，考虑到处理的性质、范围、背景和目的，可能会对自然人的权利和自由造成高风险，则控制者应在处理之前，对设想的处理操作对个人数据保护的影响进行评估。

来源： 《通用数据保护条例》(EU)2016 / 679; 第35(1)条

已公布的有关指南，指示了在处理个人数据的哪些情况下，必须进行数据保护影响评估。

在 GDPR 中，除开 DPIA，还会经常使用术语 PIA（隐私影响评估）。这两个术语描述的是相同的评估。DPIA 包含的内容及其目标在 8.3 节中会有讨论。

6.1.4 控制者—处理者合同

当控制者想将部分处理操作外包给另一方（随即成为处理者），必须签订有约束力的法律合同。这类合同的细节在 8.2 节中有描述。

6.1.5 事先协商

如果根据第35条进行的数据保护影响评估表明，控制者缺乏可环节风险的措施而使处理可能导致高风险，则控制者应在处理之前咨询监管机构。

来源： 《通用数据保护条例》(EU)2016 / 679; 第36(1)条。

与第 95 / 46 / EC 号指令要求相反，GDPR 认为处理者没有就所有处理业务向监管机构做事先协商的义务。只有在 DPIA 表明自然人的隐私或其权利与自由面临高风险时，才有必要同监管机构做事先协商。

6.2 所需的管理类型

6.2.1 记录处理活动

每个控制者，或在适用的情况下控制者的代表，都应保留其职责范围内的处理活动记录。

来源： 《通用数据保护条例》(EU)2016 / 679; 第30(1)条。

控制者的记录应包括：

（a）控制者或其代表以及数据保护官的姓名及联络资料

（b）处理的目的

（c）数据主体类别及个人数据类别的说明

（d）已经或将要向其披露个人数据的接收人类别，包括第三国或国际组织的接收者

（e）适用的情况下，向第三国或国际组织所做的个人数据传输，包括该国或该国际组织的身份（...）

（f）可能的情况下，删除不同类别数据的预期时限

（g）可能的情况下，对技术和组织安全措施的一般描述

第 30 条要求控制者保存“在其职责范围内的处理活动记录”。

当处理者根据控制者的指令执行处理活动，处理者还需要保存以下记录：

每个处理者，或在适用的情况下的处理者的代表，应保存代表控制者进行的所有类别的处理活动的记录，（...）

来源： 《通用数据保护条例》(EU)2016 / 679; 第30(2)条。

处理者的记录应包括：

（a）处理者的名称和联系方式，以及处理者所代表的每个控制者的名称和联系方式，以及在适用情况下，处理者或处理者的代表和数据保护官的姓名和联系方式

（b）代表每个控制者所做的处理的类别

（c）向第三国或国际组织所做的个人数据传输，包括该国或该国际组织的身份（...）

（d）可能的情况下，对技术和组织安全措施作一般描述

控制者和处理者的记录不一定相同。控制者可以使用多个处理者。一个处理者也可能与多个控制者签订合同。

有一个针对小规模公司和组织的义务例外：

保存所有处理活动记录的义务，不适用于雇佣少于250人的组织或企业，除非其进行的处理可能对数据主体的权利和自由造成风险，且处理不是偶发性的，或者处理涉及特殊类别的数据，或涉及与刑事定罪和犯罪有关的个人数据。

来源： 《通用数据保护条例》(EU)2016 / 679; 第30(5)条。

在实践中，此例外只在有限的范围内有用，因为它并不免除控制者证明合规的义务。

6.2.2 记录数据泄漏

控制者须记录任何个人数据泄漏事件，包括涉及个人数据泄漏的有关事实、其影响和所采取的补救措施。该记录应使监管机构能够核实对本条的遵守。

来源： 《通用数据保护条例》(EU)2016 / 679; 第33(5)条。

“涉及个人数据泄漏的有关事实”包括：

- DPO 或其他可提供更多信息的联系人的姓名和联系方式
- 数据泄漏的性质
- 涉及数据主体的类别和大致数量
- 受影响的个人数据记录的类别及大致数量
- 对自然人权利和自由可能产生的风险后果
- 已采取或将采取的应对数据泄露的后果的措施

7. 监管机构

在推出 GDPR 之前，一个紧密的“监管机构”合作系统就已经存在。它们通常被称为"数据保护局"（DPA）或其他基于当地语言的术语。

在成员国设立能够完全独立地履行义务并行使职权的监管机构，是在保护自然人个人数据处理方面的重要部分。成员国应设立一个以上的监管机构，以反映其宪法、组织和行政架构。

来源： 《通用数据保护条例》(EU)2016 / 679; 鉴于条款（117）。

欧洲经济区成员国可以设立多个监管机构。例如，德国 16 个联邦州各有一个监管机构。不过，大多数欧洲经济区成员国都是只有一个监管机构。

监管机构的独立性是这一体系的一个重要组成部分：

1. 每一监管机构在根据本条例执行任务和行使权力时应完全独立行事。
2. 各监管机构的成员在执行任务时，应根据本条例行使职权，不受任何直接或间接的外部影响，不得寻求或接受任何人的指示。
3. 各监管机构的成员应避免采取任何与其职责不符的行动，在任期内，不得从事任何不相容的职业，不论是否有酬。
4. 每个成员国应确保向每个监管机构提供有效执行任务和行使权力（包括在欧盟数据保护委员会内互助、合作和参与）所必需的人力、技术和财政资源、场地和基础设施。
5. 各成员国应确保每个监管机构选择并配备自己的工作人员，且接收来自有关监管机构成员的独立指示。
6. 各成员国应当确保各监管机构所受的财务控制不影响其独立性，并且具有单独、公开的年度预算，该预算可以是州或国家总体预算的一部分。

来源： 《通用数据保护条例》(EU)2016 / 679; 第52条）。

7.1 监管机构的一般责任

监管机构的主要职责是监督和推动 GDPR 的执行，以保护自然人在处理方面的基本权利和自由，并促进个人数据在欧盟内的自由流动（第 51 条）。

另一项重要责任是促进公众认识和了解与处理个人数据有关的风险、规则、保障措施和权利。涉及到儿童的活动应给予额外注意。

GDPR 第 57.1 条详细列出了一张冗长且开放的任务清单，因为其最后一项是"完成与保护个人数据有关的任何其他任务"。

下文将对各项任务进行总结，并进行分类。

7.1.1 监督及推动条例实施

监管机构监督 GDPR 的实施。

其监督可以是**预防性的**，办法是监测有关事态的发展或进行能对个人数据保护施加影响的调查。

监督也可以是**补救性的**，通过调查有关的处理事务，包括根据数据主体、组织或协会的投诉以及从另一个监管机构或其他公共当局收到的资料进行调查。

监管机构还可以根据第 42(7)条，对发给控制者的证书进行定期审查。

7.1.2 提供意见与提高认识

根据欧洲经济区成员国法律，监管机构可向其国会、政府以及其他机构和实体提供有关在处理过程中保护自然人权利和自由的建议。

监管机构还会就处理操作提供意见，无论是来提高控制者和处理者对 GDPR 下相关义务的认识，还是更具体地去响应控制者提出的咨询请求，或是在得到数据泄露通告后展开调查。

另一方面，应要求，监管机构还将向任何数据主体提供供有关行使 GDPR 规定权利的信息，并在适当的情况下与其他成员国的监管机构合作。

7.1.3 监管数据泄露及其他违规行为

监管机构将委会将维护一份内部记录，以登记有关的 GDPR 违犯以及基于 GDPR 第 58 条规定赋予监管机构的权力所采取过的措施。（参见 7.3 节：监管机构在执行 GDPR 方面的权力）。

7.1.4 设定标准

监管机构有责任制定标准和指引，并充当认证机构。

7.1.4.1 需要 DPIA 的处理

监管机构发布受数据保护影响评估要求的处理操作清单（参见 8.3 节：数据保护影响评估）。

7.1.4.2 行为准则与认证

监管机构应鼓励制定旨在促进正确应用 GDPR 的行为准则。监管机构应就有关协会和机构拟订或修订的行为守则提案提出意见，并核准其中能够提供充分保障的行为准则。监管机构还将对上述行为准则的监督机构进行认证。

监管机构将鼓励建立数据保护认证机制，以及数据保护印章及标识，以表明控制者和处理者遵守 GDPR 规定的处理操作，并批准认证的标准。

监管机构还将起草和公布认证机构的认证标准，以监督该认证机制。

7.1.4.3 标准合同条款与企业约束性规则及合同

监管机构可接受在控制者与处理者间、以及在可行的情况下（经控制者事先书面授权）处理者和子处理者间的约束性合同中采用标准合同条款。

监管机构可接受欧洲经济区内控制者与欧洲经济区以外尚未获得充分性认定的国家的处理者之间的合同采用标准合同条款（见 7.4：跨境数据传输）。

特别对于跨国公司和组织，监管机构可以批准具企业约束性规则（见 7.6.3 节： 企业约束性规则（BCR））。

7.1.5 与其他监管机构和欧洲数据保护主管合作。

为了促进本法规在整个欧盟内的一致适用，监管机构间应通过本节规定的一致性机制相互合作，并在适当时与委员会合作。

来源： 《通用数据保护条例》(EU)2016 / 679; 第63条。

基于前面的段落，你可能会认为，在大约 30 余个欧洲经济区国家中，有超过 50 个监管机构同时独立地制定了同样的标准。然而，事实恰恰相反。通过一致性机制，监管机构可以共享信息并向其他监监管构提供互助"以确保 GDPR 的一致应用和执行"。

它们还与欧洲数据保护委员会（也称"委员会"）分享所有相关信息，该委员会由每个成员国的一个监管机构负责人和欧洲数据保护主管或其各自的代表组成。

当监管机构作出的决定只影响其本国领土上的个人数据处理，则一致性机制不适用。而当监管机构作出决定（例如计划采用标准、指引或合同条款等），监管机构便会与该委员会分享有关资料。在大多数情况下，该委员会将与欧盟委员密切沟通，确保经过必要的讨论和修正，该提案将成为所有监管当局采用的欧洲标准。

原则上，一致性机制旨在确保国际化运营的组织在其开展业务的欧洲经济区国家中面对的是一致的合规要求。

7.2 与数据泄露有关的角色和责任

当监管机构收到数据泄露通知，他们必须能够基于一些重要标准评估个人数据泄露严重性，以及对控制者和处理者实施数据保护的方式进行评判。

显然，对数据主体所面临的风险和已经采取或需要采取的风险缓解措施的评判是最紧要的，而后才是监管机构在执行 GDPR 规则上的责任。

原则上，由控制者来负责：

- ✓ 调查数据泄漏
- ✓ 调查导致数据泄露的情况
- ✓ 评估数据主体所涉的风险
- ✓ 采取缓解措施，尽量减少对数据主体和其他有关人员的权利和自由的负面影响。

但是，监管机构拥有更广泛的权力来监督其调查，命令涉及的控制者和处理者采取其他或额外措施，以使处理业务对 GDPR 合规，甚至限制或阻止其处理。

7.3 监管机构在执行 GDPR 方面的权力

监管机构的主要职责之一是**推动**对 GDPR 的执行。除了前述的咨询权力外，监管机构还拥有很大的调查和纠正权力，以强制实施 GDPR。这包括在必要时，施以严厉的罚款。

为了确保在整个欧盟内持续地监督和执行本条例，监管当局应在每个成员国内有相同的任务和有效权力，包括调查权、纠正权和制裁权，以及授权和咨询权，特别是在自然人提出申诉的情况下，（...） 。

来源： 《通用数据保护条例》(EU)2016 / 679; 鉴于条款（129）。

7.3.1.监管机构的调查权力

GDPR 第 58(1)条赋予监管机构相当多的调查权力。他们拥有的权力包括：

a) 命令控制者和处理者，（...）提供执行任务所需的任何资料
b) 以数据保护审计的形式进行调查
c) 就已发出的证书进行审核（...）
d) 通告控制者或处理者涉嫌的违规
e) 从控制者和处理者处取得对执行其任务所需的一切个人数据及相关资料的访问

f) 根据欧盟或成员国的程序法，授权进入控制者和处理者的任何经营场地，包括调查任何数据处理的设备和手段。

7.3.2.监管机构的纠正权力

GDPR 第 58(2)条还赋予监管机构广泛的纠正权力：

a) 对预期处理有可能违反 GDPR 规定的控制者或处理者给予警告，
b) 向处理操作违反了 GDPR 规定的控制者或处理者给予谴责
c) 命令控制者或处理者响应数据主体行使 GDPR 赋予其的权利的要求
d) 命令控制者或处理者使处理操作符合 GDPR 的规定
e) 命令控制者告知数据主体其个人数据的泄露
f) 实施临时或最终限制，包括禁止处理
g) 命令更正或删除个人数据或限制处理（...） 及将该行动通知已向其披露个人数据的接收人（...）
h) 撤回授予的认证或命令认证机构撤回已发出的认证，或命令认证机构不得授予认证（...）
i) 根据每宗个案的情况，加以行政罚款，作为本段中提及措施的补充或替代
j) 命令中止向第三国的接收者或国际组织的数据流动

7.3.3 行政罚款的一般条件

每一监管机构应确保在第4、5、6款所指的违反本条规定的情况下，根据本条处以行政罚款，并确保在每一个案中都是有效的、相称的和具有劝阻性的。

来源： 《通用数据保护条例》(EU)2016 / 679; 第83(1)条。

行政罚款必须是相称的和具有劝阻性的：

7. 3. 3. 1 相称性

当管监管机构其他措施外决定处以行政罚款，必须适当考虑到具体情况。

做出决定的标准有：

- ✓ 侵害的性质、严重性和持续时间
- ✓ 处理的目的
- ✓ 受影响的数据主体的数量
- ✓ 对他们造成的损害程度。
- ✓ 控制者和处理者的责任程度
  - ■ 考虑到已实施的的技术和组织措施

与监管机构的相互合作，以纠正侵害行为并减轻侵害可能造成的负面影响，将对控制者与处理者有利。

7.3.3.2 劝阻性

罚款也应是劝阻性的，无论一个组织开展 GDPR 合规的成本如何，没有哪家公司愿意冒险无视这些规则，因为罚款将远远超出合规的成本。

然而，这样做的目的是鼓励企业遵守 GDPR，而不是在财务上摧毁它们。

罚款分为两类。

- ✓ 罚款 10.000.000 欧元，或该公司在上一财政年度的全球营业额的 2%，以较高者为准
- ✓ 罚款 20.000.000 欧元，或该公司在上一财政年度的全球营业额的 4%，以较高者为准

对于违反**控制者及处理者的义务**的行为，最高罚款额参照第一类别，为 1000 万欧元或该公司上一财政年度全球营业额的 2% ，以较高者为准。

某些类别的侵权行为将被处以更严厉的罚款：

- ✓ 违反了基本的处理原则，包括同意的条件
- ✓ 侵犯数据主体权利的
- ✓ 将个人数据传输给第三国或国际组织的接收者
- ✓ 不遵守来自监管机构的命令或对处理及中止数据流动的临时或最终限定

就这些类别而言，最高行政罚款为 2000 万欧元，最高可达该公司上一财政年度全球营业额的 4%，以较高者为准。

如果控制者或者处理者有意或者过失地，因**同一或相关的**处理操作违反本条例的若干规定，行政罚款总额不得超过最严重侵害行为所规定的数额。罚款不会根据各项相关违规做累加。

7.4 跨境数据传输

7.4.1 "一站式服务"

对跨境处理活动，或对涉及一个以上欧盟国家公民的处理活动的监督，一般规则是只有一个监管机构，称为"牵头监管机构"。这就是所谓一站式服务的原则。

牵头机构将根据条例的第60-62条，协调涉及有关监管机构的行动（例如一站式服务、互助及联合行动）。它将向与相应事项有利害关系的监管机构提交任何草案决定。

来源： WP244附件II -- 常见问题

根据鉴于条款（36），在同时涉及控制者和处理者的情况下，主管的牵头监管机构将是控制者主要机构所在成员国的有关当局。在此情况下，处理者的监管机构被视为"相关的监管机构"，并应当参与到合作程序中来。

7.4.2“跨境处理"

GDPR 区分了两种跨境处理方式：

“跨境处理”是指：
（a） 在欧盟境内多个成员国有多个经营场所的控制者或处理者在不止一个成员国的经营场所活动中对个人数据所做的处理;或者
（b）欧盟境内的控制者或处理者只在单一经营场所活动中做了个人数据处理，但该处理会严重影响或可能会严重影响多个成员国的数据主体。

来源： 《通用数据保护条例》(EU)2016 / 679; 第4（23）条。

7.4.3 跨国公司

第一种情况是在多个成员国设立机构的跨国公司。例如，ABN-Amro，一家在荷兰、比利时、法国、德国和其他成员国设有办事处的大型银行。

7.4.4 国际化运营公司

第二种情况是，在欧盟内设有一个单一的控制者或处理者，其对个人数据处理会对多个成员国的数据主体产生重大影响。例如，在荷兰东部的一家收治了来自荷兰和德国病人的医院： 其处理属于“跨境”，因为可能影响个人的健康，并涉及对医疗性（亦即特殊性）数据进行分析。

7.4.5“实质性影响"

GDPR 没有严格定义"实质性影响"的含义。然而 2016 年 12 月，"第 29 条工作组"公布的指南[1]中指出，监管机构将根据具体情况来对此进行解释，并考虑：

- ✓ 处理的背景
- ✓ 数据的类型
- ✓ 处理的目的

[1] 16/EN WP 244 http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf. 截至 2019.7.25

✓ 其他因素，例如处理是否：
- 对个人造成或可能造成伤害、损失或痛苦
- 在限制权利或机会的削夺上已经或可能产生实际效果
- 影响或可能影响个人的健康、福祉或心态平和
- 影响或可能影响个人的财务或经济状况
- 使个人容易受到歧视或受到不公平待遇
- 涉及对特殊类别个人数据或其他侵扰性数据，特别是儿童个人数据的分析
- 造成或可能导致个体行为的显著改变
- 对个人产生未料想的、意外的或不必要的后果
- 造成尴尬或其他负面后果，包括声誉损害或
- 涉及处理广泛类别的个人数据

例如在边境附近、拥有两边国家成员的划艇俱乐部，对其会员地址的处理，不会被视为对其成员产生“实质性影响"。 因此，这种处理不会被认为是“跨境处理”。

7.5 适用于欧洲经济区内数据传输的条例

7.5.1 确定牵头监管机构

（...）控制者或处理者根据第 60 条所述程序进行跨境数据处理的，由该控制者或处理者主营场所或唯一营业场所所在地的监管机构担任牵头监管机构。

来源： 《通用数据保护条例》(EU)2016 / 679; 第56条。

对于跨国性的，例如一个银行，“主营场所”是该组织中心管理机构的所在地。另一方面，如果其他场所对处理的目的和手段作决定，并有权使这些决定得到执行，那么它就成为主营场所。因此，牵头监管机构将是主营场所所在成员国的权力机构。

当控制者或处理者在欧盟内只有单一经营场所，但对个人数据的处理会对多个成员国数据主体产生重大影响的情况下，牵头监管机构是控制者该经营场所所在国家对应的监管机构。

如果处理不太可能对“跨边界”的数据主体产生实质性影响，则将由同一监管机构负责监督。但这种处理将不被视为“跨境处理”，因此不需要启动一致性机制。

7.6 适用于欧洲经济区外数据传输的条例

通常，将数据传输给第三国的接收者，只有当数据是传输到“有恰当司法管辖的区域”，或者出口数据的一方或多方已采取了合法的数据传输机制，才能被允许。

7.6.1 基于充分性认定决定的传输

如果委员会认定某第三国、或该国的某地区或该国的某个或多个特定部门、或国际组织具备充分性保护的情况下，可以向该第三国或国际组织传输个人数据。此类传输不需要任何特定的授权。

来源： 《通用数据保护条例》(EU)2016 / 679; 第45(1)条。

“充分性认定”是欧盟委员会通过的一项决定，认定某第三国可以通过其国内法或其作出的国际承诺确保个人数据得到充分程度的保护。这种认定的效果是个人数据可以从欧盟成员国和欧洲经济区成员国（挪威、列支敦士登和冰岛）传输至该第三国，而无需要任何进一步的保障措施。

欧盟委员会根据第 95 / 46 / EC 号指令作出了充分性认定，承认安道尔、阿根廷、加拿大（的商业组织）、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士、美国[2]和乌拉圭提供了充分的保护。

在 GDPR 生效时，这些认定大多数已经执行，但第 45(4)条中要求委员会监督可能影响这些认定运作的第三国和国际组织的发展。如果委员会认为第三国、某地区或一个国际组织不再能确保适当程度的保护，它可以撤销、修改或中止该认定。

7.6.2 基于适当安全保障的传输

在缺少充分性认定的情况下，控制者或处理者应采取措施，通过对数据主体采取适当的安全保障措施来弥补第三国所缺乏的数据保护。

这类适当的安全保障可能包括：采用企业约束性规则、欧盟委员会通过的标准数据保护条款、监管机构采用的标准数据保护条款或监管机构授权的合同条款。

（...）这些安全保障应确保在欧盟境内的处理遵守数据保护要求和数据主体权利，包括欧盟或第三国是否有可执行的数据主体权利以及有效的法律救济，包括是否可取得有效的行政或司法救济以及主张的赔偿。

（...）可由公共当局或机构向第三国的公共当局或机构，或与具备相应职责的国际组织进行数据传输，包括基于嵌入行政安排的规定，例如谅解备忘录来提供可执行及有效的数据主体权利

来源： 《通用数据保护条例》(EU)2016 / 679; 鉴于条款（108）。

[2] 有关美国的充分性决定限于“隐私盾网络”（参见 7.5.4 节）。

当数据传输发生在公共机构间，公共当局必须确保符合 GDPR 的要求。其他情况要求要么遵循已审核的标准，要么遵守由监管机构已采纳的保护条款。

7.6.3 约束性企业规则（BCR）

企业团体或从事联合经济活动的企业集团，可利用经批准的具有约束力的企业规则，来做从欧盟到同一企业团体或从事联合经济活动的企业集团的跨国传输，前提是此类公司规则包含所有关键原则和可执行的权利，以确保个人数据的各类传输具有适当的安全保障。

来源： 《通用数据保护条例》(EU)2016 / 679; 鉴于条款（110）。

主管监管机构批准一套企业约束性规则的基本要求是：

- ✓ 具有法律约束力
- ✓ 适用于该群体的每一个成员，包括其雇员，并由其执行；
- ✓ 在处理个人数据方面明确赋予数据主体可执行的权利；
- ✓ 满足 GDPR 第 47(2)条规定的要求。

这个相当长的列表特别指出，BCRs 必须至少规定：

- ✓ 数据传输、数据类别、处理类型及其目的
- ✓ 受影响的数据主体类型和对第三国的界定
- ✓ 通用数据保护原则的应用，以及向不受企业约束性规则约束的机构传输的要求
- ✓ 数据主体在处理方面的权力和行使这些权利的方式
- ✓ 在成员国领土设立的控制者或处理者，对于其不在欧盟设立的成员违反企业约束性规则承担责任
- ✓ 与监管机构的合作机制，以确保集团的任何成员遵守（...）

7.6.4 未经欧盟法律授权的传输或披露

GDPR 限制向第三国，即欧洲经济区以外的国家传输个人数据。

法院或仲裁庭的任何判决以及第三国行政当局要求控制者或处理者传输或披露个人数据的任何决定，只有在基于请求国与欧盟或成员国之间有生效的国际协定（...） 的情况下，才能予以承认或执行，但不得损害本章中关于传输所需要依照其他理由。

来源： 《通用数据保护条例》(EU)2016 / 679; 第45(1)条。

7.6.5 适用于欧洲经济区和美国之间数据传输的条例

如 7.5.2 节所述，欧盟委员会可以作出“充分性认定”以承认一个国家或一个国家的一部分具备充分的数据保护（GDPR，第五章）。但是由于美国数据保护法与 GDPR 以及之前的指令有很大的不同，因此对于美国，无论是对于其国家或其地理区域都尚未给予充分性认定。

取而代之的是，欧盟委员 2016 年 7 月颁布的 2016 /1250 号决议来承认美国商务部实施的欧盟-美国隐私盾计划所提供保护的充分性。

在一份新闻稿（2016 年 7 月 12 日 IP-16-2461）中，欧盟委员会描述了欧盟—美国隐私盾保护的原则如下：

对于处理数据公司的严格义务：

（...）美国商务部将定期对参与公司进行更新和审查，以确保公司遵守他们自己提交的规则。如果公司在实践中不遵守规定，他们将面临制裁，并被从名单上除名。收紧向第三方传输数据的条件，将保证从隐私盾计划内的公司传输数据时有同等程度的保护。

对于美国政府获取数据时明确的安全保障和透明性义务：

美国政府向欧盟保证，公共当局在执法和国家安全方面的数据获取，受明确的限制、安全保障和监督机制的约束。欧盟公民也将首次从该领域的赔偿机制中获益。根据欧美隐私盾协议，美国已经排除了对传输到美国的个人数据的无差别大规模监视。国家情报主管办公室进一步澄清，大量收集数据只能在特定的先决条件下使用，需要尽可能有针对性和聚焦。它详细说明了在这种特殊情况下使用数据的现有保障措施。美国国务卿通过国务院内的监察员机制，在面向欧洲的国家情报领域建立了一种补救可能性。

有效保护个人权利：

任何认为他们的数据被隐私盾计划所滥用的公民，将受益于几种可利用和负担得起的争端解决机制。理想情况下，申诉将由公司自己解决；或免费提供替代性争议解决方案。个人也可以找到它的国家的数据保护当局，通过该当局与联邦贸易委员会的合作，确保欧盟公民的申诉得到调查和解决。如果一个案件没有通过任何其他手段解决，作为最后手段，将有一个仲裁机制。欧盟公民在国家安全领域的补偿可能性将由独立于美国情报部门的监察员来处理。

年度联合审查机制：

该机制将监测“隐私盾”的运作情况，包括为执法和国家安全目的查阅数据的承诺和保证。欧盟委员会和美国商务部将执行审查，并协理美国和欧洲数据保护局的国家情报专家。委员会将利用所有其他可用信息来源，并向欧洲议会和理事会发布一份公开报告。

数据保护实践

8. 更高标准层面

8.1 基于设计和默认的数据保护

在确定处理手段以及在处理数据时，控制者均应采取适当的技术和组织措施，例如假名化，以有效地执行数据保护原则，如数据最小化，将必要的安全措施纳入处理过程，以满足本条例的要求并保护数据主体的权利

来源：《通用数据保护条例》(EU)2016 / 679; 第25(1)条。

根据本条，GDPR 使**基于设计的**数据保护原则成为一项**法律要求**，而不单纯是一种履行数据安全义务的有效方法。控制者需负责实施一套完整的端对端**适当的**技术和组织措施。

此外，GDPR 在第 25(1)条中指出，需采取此套适当的技术和组织措施，将必要的安全保障纳入处理工作（...）以保护数据主体的权利。这样就定义了数据安全原则与隐私，连同与个人的权利及自由之间的法定关系。

第 25 条第 2 款要求控制者采取适当的技术和组织措施，以确保**默认情况下**只对一个特定的处理目的来处理个人数据。这一条也应用于个人数据收集的数量、处理的程度、储存时长和可获取性。

8.1.1 基于设计的数据保护的七项原则

通过设计保护数据的想法是由加拿大安大略省前信息和隐私专员 Ann Cavoukian 博士提出，在一份涉及相关原则的出版物中她写到：

基于设计的隐私是我在90年代提出的一个概念，旨在解决信息和通信技术以及大规模网络数据系统日益增长的系统性影响。基于设计的隐私提出了一种观点，即未来的隐私不能仅仅通过遵守监管框架来确保，隐私保障必须成为一个组织的默认操作模式。

来源：Ann Cavoukian，2011年《基于设计的隐私：7项基本原则》。

GDPR 更愿意使用“基于设计（和默认）的数据保护”，正如我们在下面几段中的所用。

8.1.1.1 主动而非被动；预防而非补救

基于设计的数据保护的特点是采取主动的而非反应性的措施。它在隐私侵犯发生之前就预测并防止它。基于设计的数据保护不会等待隐私风险的出现，也不会提供解决隐私违规的补救措施——它的目的在于**防止**它们的发生。简而言之，基于设计的数据保护是在事前而非事后进行的。

8.1.1.2 数据保护作为默认设置

我们都可以确定一件事——默认的规则。基于设计的数据保护旨在提供最大程度的隐私，确保个人数据在任何特定的 IT 系统或业务实践中均受到自动的保护。即使一个人什么都不做，他们的隐私仍然完好无损。数据主体不需要采取任何行动来保护他们的隐私。默认情况下，隐私与数据保护内置于系统中。

8.1.1.3 嵌入设计的隐私

基于设计的数据保护已嵌入到 IT 系统的设计和架构以及业务实践中。事实上它不是作为一个被固定的配件。而是将隐私变成交付核心功能的重要组成部分。数据保护是整个系统的一部分，且不会削弱系统的功能。

8.1.1.4 完整功能——正和，而非零和

基于设计的数据保护旨在以“正和”和“双赢”的方式满足所有合法利益及目标，而不是采用过时的零和的方法来做不必要的折中。基于设计的数据保护避免了错误二分法（例如隐私与安全）的托词，而表明两者完全有可能兼得。

8.1.1.5 端到端安全——完整生命周期保护

基于设计的数据保护在收集信息的第一个要素之前就已经嵌入系统，并安全地扩展到涉及数据的完整生命周期中。这意味着从开始到结束，强有力的安全措施都对隐私至关重要。这样就可以确保所有数据都被安全地保存，然后在流程结束时，及时安全地销毁。因此，基于设计的数据保护保证了从头到尾的、安全的端到端信息生命周期管理。

8.1.1.6 可见性和透明度——保持开放

基于设计的保护数据旨在向所有利益相关方保证，无论涉及哪种业务实践或技术，它实际上都是按照所声明的承诺和目标运作的，并受独立地核查。对于用户和供应商来说，它的构成部分和操作始终是可见的和透明的。请记住，信任，但要核查。

8. 1. 1. 7 尊重用户私隐——以用户为中心

最重要的是，基于设计的数据保护要求架构师和执行者通过提供诸如严格的隐私默认设置、恰当的提示和赋予用户友好的选项等措施来保证个人利益的至上。确保以用户为中心。

8.1.2 基于设计和默认的隐私，应用其有关原则的好处

在英国信息委员办公室（ICO）的网站[3]写道：

采用基于设计的数据保护方法是最小化隐私风险和建立信任的重要工具。从一开始就在设计项目、流程、产品或系统时考虑隐私，可以带来以下好处：

- ✓ 尽早发现潜在问题，解决这些问题往往更简单，成本也较低
- ✓ 提高整个组织对隐私和数据保护的认识
- ✓ 各组织更有可能履行其法律义务，更少可能违反《数据保护法》。
- ✓ 有关行动更少可能侵犯隐私，并 对个人产生负面影响。

8.2 控制者和处理者之间的书面合同

GDPR 第 25 条要求控制者采用适当的技术和组织措施，并确保在处理过程中这些预防措施能够持续，这实际上是执行基于设计的数据保护原则中的一项：端到端的安全。

当一个处理者参与处理或部分的处理，理应有一份书面合同，这正是 GDPR 所要求的。

处理者处理数据应遵守合同或欧盟及其成员国的相关法规，该合同或法律法规应对处理者有约束力，并明确处理的主题、期限、性质和目的、个人数据的类别、数据主体的分类以及控制者的权利义务。（…）

来源：《通用数据保护条例》(EU)2016 / 679; 第28(3)条。

8.2.1 书面合同的条款

第 28 条第 3 款进一步规定：合同（或其他法律行为）应特别规定处理者：

a) 只根据控制者的书面指示处理个人数据，包括向第三国或国际组织传输个人数据的情况（...）

[3] https://ico.org.uk/，截至 2017. 4. 25

b) 确保被授权处理个人数据的人员承诺保密或承担适当的法定保密义务
c) 采取根据第 32 条（处理的安全性）规定的所有措施
d) 遵守引入其他处理者的条件
e) （...）在可能的情况下，通过适当的技术和组织措施，协助控制者履行其在数据主体要求行使其权利时作出响应的义务（...）
f) 根据处理的性质和处理者可获得的信息，协助控制者确保遵守第 32 至 36 条规定的义务
g) 基于控制者的选择，在与处理有关的服务结束后，删除或返还给控制者所有的个人数据，并删除现有的副本，除非欧盟或成员国法律要求个人数据的存储
h) 向控制者提供一切必要的资料，以证明其遵守了本条规定的义务，允许和协助审计，包括由控制者或其授权的其他审计员进行的审查。

8.2.1.1 示例

下表显示了控制者和处理者之间的这种数据处理协议中内容的示例：

内容表	GDPR 索引
协议的范围和目的	第 4(2)条，定义： 处理
协议所涵盖的数据	第 4(1)条，个人数据 第 9 条/鉴于条款第 10 条，个人数据的特别类别（敏感数据）
数据处理的一般安全和保障	第 32 条，处理的安全性
技术及组织措施	第 28 条(3)(a)... (h)款
监督信息安全和数据保护	第 35 条，数据保护影响评估
信息安全侵害和个人数据泄露	第 33 条(2)款，向监管机构通报个人数据泄露
更正、删除和阻止/协助控制者的特定义务	第 32...36 条
与其他数据处理者（子数据处理者）的协议	第 28 条(2)和(4)款：子处理者
数据传输	鉴于条款第（112）， （113）款 第 47 条，约束性企业规则 第 49 条，对具体情况的克减 第 5 章，向第三国或国际组织的传输
处理者的进一步义务	第 39 条，数据保护官的任务； (1)(b)款...参与处理作业工作人员的认识提高与培训
控制者的控制权	第 4 条(7)，控制者 第 8 条(3)(f)款，协助控制者
返回及删除个人数据	第 28 条(3)(g)款，删除或返还
保密责任	第 28 条(3)(b)款，保密
期限	第 28 条(3)款，"... 合同...处理期限。"

	第 5 条，关于处理个人数据的原则，(1)(e)款，储存限制
优先级	在条款冲突的情况下，GDPR 优先
签名	

8.3 数据保护影响评估（DPIA）

"基于设计的数据保护"的第一项原则要求控制者，事实上是任何处理个人数据的人，在隐私侵害事件发生前就进行预防。

GDPR 第 35 条列入了这一原则：

如果某种处理，特别是使用新技术，考虑到处理的性质、范围、背景和目的，可能会对自然人的权利和自由造成高风险，则控制者应在处理之前，对设想的处理操作对个人数据保护的影响进行评估。存在相似较高风险的一系列近似处理操作可统一进行一次评估。

来源：《通用数据保护条例》(EU)2016 / 679; 第35(1)条。

GDPR 不需要为每一个处理操作执行 DPIA。《数据保护影响评估指引》和就处理是否"可能导致高风险"的准则（17/ EN WP248）中，第 29 条工作组详细说明了 DPIA 是什么，开展 DPIA 何时是强制或建议的：

- ✓ DPIA 是一套程序，旨在描述处理过程，评估处理的必要性和相称性，并帮助管理由于处理个人数据而对自然人的权利和自由造成的风险。
- ✓ 只有在处理可能对自然人的权利和自由造成高风险的情况下，才需要进行 DPIA（第 35(1)条）。

GDPR 并没有明确定义评判的标准是什么，但是提供了一些实例：

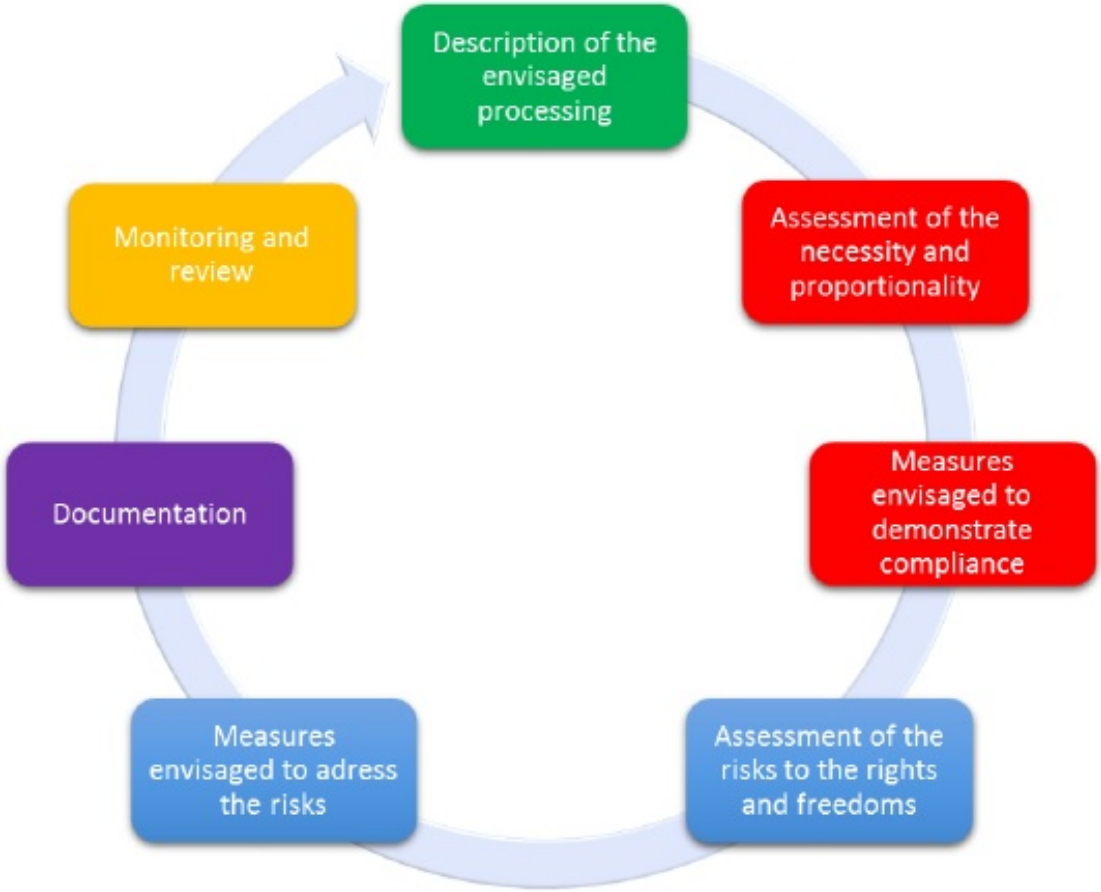
（a）基于自动化处理（包括剖析）对自然人的个人情况进行系统、广泛的评估，并基于该评估做出对该自然人产生法律效力或类似重大影响的决定;
（b）对第 9 条第 1 款所述的特殊种类的数据，或第 10 条所述的与刑事定罪和犯罪相关的个人数据进行大规模处理;或
（c）对公共区域进行大范围的系统监控。

来源：《通用数据保护条例》(EU)2016 / 679; 第35(3)条

一个 DPIA 可以针对单个处理操作或一组类似的处理操作。这意味着只要充分考虑到处理的具体性质、范围、背景和目的，就可以**使用单一的 DPIA 来评估风险相似的多种处理作业**。这种情形意味着近似的技术被用于收集同样类型的数据以达到相同的目的。

DPIA 应**在处理之前**进行（第 35(1)条和第 35(10)条，鉴于条款第 90 和 93 款）。 这与基于设计和默认原则的数据保护相一致（第 25 条和鉴于条款第 78 款）。

即使某些处理操作仍然未知，DPIA 也应在设计处理操作时就**尽早开始**。随着 DPIA 在整个项目生命周期中的更新，它将确保数据保护和隐私始终被考虑，并推动制定解决方案以促进合规。随着处理进程的推进，可能需要重复评估个别步骤，因为某些技术或组织措施的选择，可能会改变处理过程所造成风险的严重性或可能性。



一旦实际开始处理，就可能需要更新 DPIA，但这并不是推迟或不执行 DPIA 的正当理由。在某些情况下，DPIA 将是一个持续的过程，因为处理操作是动态的并且不断变化的。因而实施 DPIA 是一个持续的过程，而不是一次性的实施。[4]

[4] 图片来自于《数据保护影响评估（DPIA）指南》，WP29 文件 17 /EN/ 248。

8.3.1 DPIA 的目标

开展 DPIA 的原因有很多，例如 “基于设计的数据保护”原则中的预防思想、记录遵守情况的义务等。具体而言，一个 DPIA 将有助于：

- ✓ 防止因流程的更改、系统的重新设计或项目的终止带来的高昂代价
- ✓ 减少监督和执法可能带来的的不良后果
- ✓ 提高数据质量
- ✓ 改善服务提供
- ✓ 改善决策
- ✓ 提高组织的隐私意识
- ✓ 提高项目可行性
- ✓ 改善与隐私和个人数据保护有关的沟通
- ✓ 在处理个人数据和尊重隐私方面加强数据主体的信心

8.3.2 DPIA 报告的主题

GDPR 规定了 DPIA 的最低要求（第 35 条(7)款，鉴于条款第 84 和 90 款）：

- ✓ 关于所设想的处理操作和处理目的的说明
- ✓ 对处理的必要性和相称性进行评估
- ✓ 对数据主体的权利和自由所面临的风险的评估
- ✓ 计划采取的措施：
  - 消除风险
  - 证明合规

8.4 数据生命周期管理（DLM）

无论数据是是在组织内部产生，还是由组织通过第三方（客户、供应商、合作伙伴）收集，有效保护数据的唯一方法就是了解它。它是否包括任一类别的个人数据，例如，客户资料、雇员资料、敏感通讯、个人身份信息、健康信息或金融数据？在这些情况中，GDPR 可能都适用，从收集数据一开始就需要适当的保护。需要将结构化的隐私和安全嵌入到任何项目的基础架构中去。但事实上数据在其整个生命周期中都会发生变化，并且经常被存储多年（无论是为了记录还是以防万一）。而因为有了 GDPR，后者正在成为一个奢侈的习惯。

8.4.1 数据生命周期管理（DLM）的用途

数据生命周期管理（DLM）是一个过程，它帮助组织管理整个生命周期的数据流——从创建、使用到共享、存档和删除。

在整个信息生命周期中准确跟踪数据是一个敏锐性的数据保护战略的基础，有助于确定在什么环节实施安全控制。

8.4.2 了解数据流

GDPR 的各项要求需要公司知道：

- ✓ 其数据，特别是个人数据的确切位置
- ✓ 收集或创建这些数据的用途
- ✓ 必须保留这些数据的原因
- ✓ 必须在何时或何种情况下予以删除。

8.4.2.1 数据收集

从一开始就必须牢记，为了预期的处理目的，哪些个人数据是必要的。GDPR 要求保存个人数据要有具体的理由，因此在任何时候都必须清楚和能够容易证明：

- ✓ 收集信息的用途
- ✓ 在何时向数据主体通报收集情况和处理目的
- ✓ 是否为拟进行的处理取得了同意
- ✓ 该同意是否仍然有效（和未撤回）
- ✓ 处理还有什么其他的合法理由

在实践中，每一条信息都需要许多标签来说明它存在的原因，以及它需要保留多久。

8.4.2.2 权限结构

任何数据收集，特别是个人数据的收集，都需要一个权限结构，明确定义哪些员工因为其在组织中的角色，需要去查阅获取哪些个人数据。

然而事物总是在变化。一个好的程序必须不断地评估和审查谁需要访问什么类型的信息。控制者和处理者应该与它们的 IT 合作方一起，使整个企业系统的控制自动化。他们必须使员工更容易做正确的事情，而非错误的事情。他们必须避免员工因为由于简单的疏忽而使他们的行为带来负面的影响。

一旦权限结构就绪，就必须通过定期和持续的评估来维护。

8.4.2.3 建立留存与删除规则

GDPR 的关键原则之一是数据最小化：控制者和处理者有义务确保个人数据足够、相关且限于其处理目的的需要（第 5(1)（c）条）。在实践中，它可以在留存什么数据、为什么留存以及在安全的方式下处理哪些数据之间实现持续的平衡。

储存个人数据对任何组织来说都是一个负担。为了保证数据的安全性、完整性和最新性，需要付出很大的努力，而且还需要更多的努力来回应数据主体提出的关于提供处理其数据的信息，以及处理数据主体对其权利的主张。此外，个人数据泄露的威胁总是存在，连同由此产生的响应程序、数据主体的风险以及公司遭受损害的风险，如名誉损失、补救措施的成本和可能的罚款。

在一定时间内留存个人数据伴有许多法律义务。你可以想想诸如销售和金融交易，担保或人力资源信息，如简历、付款记录、税务信息中涉及的客户信息登记。

良好的数据生命周期管理：

- ✓ 为信息系统中的数据流管理提供工具
- ✓ 从收集或生成数据的那一刻起追踪数据，直到它没有合理的留存理由而被删除。

8.5 数据保护审计

GDPR 中的一些条款提到审计是监管 GDPR 合规的方法之一。例如，在数据保护官（DPO）的任务中：

数据保护官应至少承担以下任务：监督本法规以及其他欧盟或成员国的数据保护规定的遵守情况，监督控制者或处理者对其在保护个人数据方面政策的遵守、包括对参与处理操作工作人员的职责分配、认识提高和培训，以及相关的审计;

来源： 《通用数据保护条例》(EU)2016 / 679; 第39(1)(b)条。

除第 39 条，第 47(2)(j)条要求企业约束性规则应具体规定有关审计工作，以评估那些用以确保企业约束性规则得到遵守的有关机制。

第 58(1)(b)条赋予监管机构以数据保护审计的形式进行调查的权利。

8.5.1 审计的目的

数据保护审计程序的目的是定期测试、评估和评价有关技术和组织措施的有效性，以确保遵守 GDPR，包括处理的安全性。

通常，审计会发现需要加以解决的隐私政策中的**不足**，以加强数据隐私治理。

至少，审计也将通过使个人数据保护成为“本周主题”，从而提高整个组织的意识。

一般来说，可以将隐私审计划分为两种：： 一种是充分性审计，另一种是合规性审计。

8.5.1.1 充分性审计

充分性审计的目的是：

- ✓ 确保本组织的数据保护政策适用于实际发生的所有个人数据处理的实例
  - ■ 包括容易被遗忘的历史数据集、备份、过时设备等
- ✓ 评估这些政策是否足以满足 GDPR 的要求，以及其他可能适用的数据保护法律和条例的要求
  - ■ 既包含欧洲经济区内的也包含欧洲经济区外的外的

这需要对整个企业的数据流有完整的理解和映射，而它不止是审查整个生命周期内影响个人数据处理的所有政策、程序、业务准则和指南。充分性审计应当在公司内部以及所有涉及的第三方（例如处理者）都开展。

8.5.1.2 合规性审核

在完成充分性审计之后，下一步可能是（或更应该是）合规性审计，以确定该组织是否实际遵守了充分性审计期间确定的政策和程序，是否有因充分性审计而得到的改进。

合规性审计要求调查各业务单位、部门之间以及与第三方打交道时，个人数据是如何**在实际中**处理的。

全面的合规性审计还应审查以下要素：

- ✓ 组织是否提供数据隐私合规培训
- ✓ 员工是如何得以了解数据隐私政策的
- ✓ 如何处理关于违反政策的投诉。

合规性审计的深度将取决于企业意识到的违规和数据泄露给它带来的风险。

8.5.2 审计计划的内容

- ✓ 审计方案的制定（规划）：
  - o 联系人，目的，时限。
- ✓ 确定审计方法和范围：
  - o 充分性审计还是合规性审计

- 以特定部门（例如人力资源）为对象的纵向（功能性）审计，或
- 横向（过程）审计；从一端到另一端追踪特定的过程
- 审计范围（数据保护治理、记录管理、访问管理及数据安全、数据保护培训及数据保护认知等）

✓ 准备工作，收集这些领域的证据，包括：
- 委托书
- 合同，如控制者-处理者合同，BCRs，保密协议等
- 处理描述；工单，通知
- 培训资料、宣传页等

✓ 执行审计

✓ 报告：
- 总体结论
- 有良好实践的领域
- 有待改善之处

✓ 跟进

8.6 与使用数据、营销和社交媒体相关的应用实践

8.6.1 在营销活动中使用社交媒体信息

就在不久前，仍有这样三种方式可以让公众注意到一个供应商试图销售的产品或服务：

✓ 购买昂贵的广告
✓ 请求主流媒体讲述他们的故事
✓ 雇佣大量销售人员直接向人们推销产品。

这些方式都不是很有效。这三个方式都是基于“打断人们他们正在做的事情”，希望他们能看到产品并且想：“这就是我一直在寻找的”，如果是这样，他们就会记得是谁在打广告，在哪里找到产品。

使用互联网，则有让你的产品获得关注的更好选项。从生产者和消费者的角度来看，人们成为了“生产消费者（prosumers）[5]”，通过批评来设计，通过花钱来消费。建立网站，写博客，在社交媒体上发布内容和多媒体的内容（图片、声音、视频）变得很容易。不止是供应商，实际上所有人都可以发布自己的内容，那些消费者愿意购买的内容。

通过社交媒体，每个人都可以与世界上任何地方使用同一社交媒体的其他人联系。 仅 Facebook 一家就拥有超过 15 亿的用户，一个广阔的全球市场正在敞开大门。

[5] 更多信息参见：https://en.wikipedia.org/wiki/Prosumer

随着数字时代的这些变化，业务正在变的“多渠道”和可交互。供应商像记者一样描写他们的产品，人们对此的反应表明他们喜欢看到什么，喜欢什么被生产，以及什么被提供。当然，如果他们不喜欢，他们也会毫不犹豫地告诉全世界，而且相当直言不讳。

最后，一种新的销售理念正在形成。许多人发现其他人，尤其是朋友对他们正寻求产品的看法很重要。“76%的朋友喜欢这个产品”的信息被证明是一种购买动机，即使没有办法去确认，但我们似乎都相信它。

人们可以被分成品味相似、兴趣相似的群体。在浏览网络商店的时候，我们都看到过类似这样的评论：<你刚刚看过的产品>的买家也买了：<这些其他产品>。 在实践中，这已被证明是一种非常有效的 “销售促进”，只要你的品味和兴趣与其他买家相似。

8.6.2 在营销领域使用互联网

为了使这种新型与更数字化的经济发挥作用，公司需要了解潜在买家的信息。实际上这意味着他们需要尽可能多的消费者信息。它是什么类型的消费者？ “野外宿营” 型，需要高质量的户外装备和衣服？“我想要最新的技术”型？或者是“最好的性价比”型，抑或更确切地说是“保证最低价格”的买家？

这样的分析需要了解有关人员及其行为的大量数据。而这些公司是怎么得到这些信息的？

8.6.3 Cookies

Cookie 是存储在用户计算机上的一个（通常很小的）文本文件。最常见的 cookies 有：

- ✓ 会话型 cookies
- ✓ 持久型 cookies
- ✓ 跟踪型 cookies

8.6.3.1 会话型 cookies

会话型 cookies 允许用户在网站内被识别，因此用户做的任何页面更改，或选择的条目及数据都会被逐页记录下来。最常见的例子是任何网店中有的购物车功能。每当商品被选中，其选择都存储在会话型 cookie 中，且在用户退出登录之前都会被记住。

当登录到一个网站时，用户计算机内存中的会话型 cookie 会保留登录成功的信息，因为网站没有其他办法记录你已登录。当离开网站，通常意味着关闭浏览器时，会话型 cookie 会从用户的电脑内存中删除，相应地，用户就会退出。

8.6.3.2 持久型 cookies

持久型 cookie 将保留在用户的硬盘中，直到用户删除或者直到它们过期。持久型 cookie 可以向作为重复访问者的用户提供简单的服务。例如，保留用户的语言选择。当用户稍后重新访问该网站时，它将根据 cookie 中的信息按前一次访问中选择的语言来提供内容。

这种类型的 cookie 可以使网站访问者的体验更加个性化。比如一个订票的网站，有人在上面订了一个飞往英国湖区的廉价航班。为了使（包括财务和航空公司的）交易获得成功，用户必须填写个人信息（姓名、地址、护照号码、信用卡信息）。下一次用户访问网站时，这些信息的组合能生成一个更个人的问候，比如“早上好<名字>”，还可以提供其他旅行，旅行保险，更好的徒步装备，旅行包等方面的信息。所有这些都是基于这次（以及可能更早的）预定行程所收集到的信息。

没有必要在 cookie 中保存大量信息。事实上，唯一标识符足以识别用户（或至少是该用户的设备或浏览器），并将该标识符与数据库连接。

8.6.3.3 跟踪型 cookies

跟踪型 cookie，通常被称为**第三方** cookie，它是由网站从其他域名，而非该用户正在访问的域名处获得，并放置到用户的硬盘上的。

与普通 cookie 一样，放置在用户计算机上的第三方 cookie 可以保存用户的一些信息，以备日后使用。然而，第三方 cookie 通常由该网站所加入的的广告网络所设置。

这种 cookie 的目的是跟踪一个人正在访问的页面，建立基于其兴趣的个人画像。用户的画像信息可被添加到在其所在网络中的其他网站中去。它并不链接到与网站上已知的个人信息，仅是用于使广告与用户画像尽可能相匹配。

8.6.4 其他画像信息："免费"服务的价格

Facebook 和 Google 几乎知道其免费产品用户的所有信息。

当您使用我们的服务时，我们会搜集您所提供的内容和其他信息，包括当您注册一个账户，创建或分享，以及给人发送消息或与他人交流。这里包括您提供的内容及相关的信息，比如照片的拍摄地点或文件创建的日期。我们还会收集关于您如何使用我们的服务的信息，比如您看到或参与的内容类型，或者您活动的频率和持续时间。

来源： Facebook 隐私政策

谷歌也是如此。通过数十亿人使用他们的搜索引擎，再加上来自 LinkedIn，谷歌地图，博客文章，谷歌知道人们正在做哪些活跃的搜索或购买，以及他们寻找它们时所使用的词语。 他们知道每个用户可能很快会购买什么，以及现在、今天晚些时候、明天或其他时候他们需要购买什么。

因为谷歌有我们在哪里，我们是谁，我们将要在哪里，我们将要做什么的信息。他们知道很多关于我们是谁，我们花了多少钱，我们以什么为生，我们的人口数据（年龄、性别、宗教、收入、教育等等），我们生活在哪里，我们的朋友是谁，我们在工作之外做什么，我们为谁投票，我们消费哪些电视、播客、音乐或其他娱乐，以及更多。

谷歌也知道这些事情是如何随着时间的推移而改变的。这使得他们能够在个人和集体层面上发现趋势并预测行为。简而言之，他们拥有公司最大化营销所需的信息，也是在你需要时就能为提供所需产品或服务的有关信息。

8.6.5 数据保护的观点

于 2017 年 1 月发布的，旨在废除现行的指令（2002/58/EC）而拟立的《隐私和电子通信条例》[6]，详细规定了电子通信中保护个人数据的有关规则。

拟议的修改将使电子隐私指令（e-Privacy Directive）与 GDPR 保持一致。根据该提案中第 27 条，该条例原计划是于 2018 年 5 月 25 日与 GDPR 同时生效。然而，欧盟理事会内部仍几乎每个月都在讨论法律案文的细节。因此，预计在 2020 年之前不会最终实施这项规定。

《隐私和电子通信条例》特别着眼于有关通信数据和元数据的处理。第 8 条涉及“保护储存在用户终端设备的信息以及与用户终端设备有关的信息”，比如 cookies，也包括间谍软件、隐藏标识符、网络 bug 和设备指纹等。

8.6.5.1 Cookies

除开终端用户所关注的以外，使用终端设备的处理和储存能力，以及从最终用户终端设备收集信息，包括关于其软件和硬件的信息都应被禁止，除非有下列理由：

来源：（草案）关于隐私和电子通信的条例（2017 / 0003）第8(1)条。（截至2017.6.5）。

例外情况如下：

(a) 只为在电信网络上传送电子通讯的目的，或
(b) 最终用户已给予同意，或
(c) 对于最终用户请求的信息服务来说是必要的

[6] 欧洲议会和欧洲理事会关于在电子通信中尊重私人生活和保护个人数据的提案，同时废止了第 2002 / 58 / EC 号指令（隐私和电子通信条例）

(d) 如果对网络受众的测量是必要的，且这种测量是由最终用户所请求的信息服务提供者执行的

会话性 cookie 通常适合于(a)、(c)或(d)，因此可以在未经同意的情况下储存，例如之前讨论过的购物车。

对于其他 cookie，需要在 GDPR 中所定义的“同意”，该同意必须是自由给予、具体、知情、有效和明确的。该提案中新的内容是，最终用户可以通过他们的浏览器设置表达同意（或不同意）。这将有助于减少过多的横幅提示与弹窗确认。

8.6.5.2 剖析

正如鉴于条款（72）所明确指出的， GDPR 无疑适用于前述的剖析（用户互相）;。 因此，数据主体有权反对以下处理：

在为直接销售目的来处理个人数据的情况下，数据主体应有权反对这种处理（包括与这种直接销售有关的剖析），无论是在初期还是后续的处理，在任何时候，无论是否免费。应当明确提请数据主体注意这项权利，并与其他的信息分开和明确地提出。

来源： 《通用数据保护条例》(EU)2016 / 679; 鉴于条款（70）。

作为 GDPR 的一个新要求，相关权利尤其是检查和纠正的权利，将给数据主体赋权更多：

数据主体应有权查阅有关其自身的已被收集的个人数据，并以合理的频率和简便的方式行使该查阅权，以便了解并确认该数据处理的合法性。

上述权利包括数据主体有权查阅涉及其健康的有关数据，例如其医疗记录中有关诊断、检查结果、主治医师的评估及提供的任何治疗或诊疗等。

每个数据主体应有权了解并获知个人数据处理的用途、处理期限（可能的情况下）、个人数据的接收者、任何自动化处理个人数据的逻辑以及该等处理的后果（至少在以剖析为基础进行处理的情况下）。

在可能情况下，控制者应能够提供安全系统的远程访问，允许数据主体直接查阅其个人数据，但该等查阅权不得对他人的权利或自由（包括商业机密或知识产权，特别是保护软件的版权）产生不利影响。但不得因前述限制而拒绝向数据主体提供所有信息。

当控制者处理涉及数据主体的大量信息时，控制者应能够在提供有关信息前，要求数据主体明确其请求所涉及的信息或处理活动。

来源： 《通用数据保护条例》(EU)2016 / 679; 鉴于条款（63）

仍然会有很多“免费”的服务，提供内容或其他免费的产品或服务，只要用户同意收集关于他们及其兴趣和品味的信息，用以“选择适当的广告”。GDPR 不会改变这一现状，但至少会给我们纠正这些信息的机会。

对于提供新闻通讯或其他免费服务的公司，数据主体应谨慎地向其披露信息。如上所述，一旦数据主体意识到一家公司在跟踪他们的行为，反对这种处理应该是受到支持的。

问题的关键在于，大多数人习惯于同意冗长的声明，而实际上并不阅读它们。GDPR 禁止冗长、不可读的声明，并要求用简单、清晰的语言解释收集的个人数据将用于什么目的。

8.7 大数据

为建立前面几段中所述的用户画像而针对客户（或者说——使用互联网的每一个人）所做的大量信息的处理，正是对本文第一段中评论的注解。

挑战来自于在保护个人自由与支持整个欧洲自由贸易之间找到一种平衡。

人们有理由怀疑“隐私”是否真的有未来。然而 GDPR 明确指出，欧盟委员会将严肃履行它在鉴于条款第(1)和(2)款中所述的义务：

> 无论人们的国籍或居住地在哪，在个人数据处理方面保护自然人的有关原则和规则，都应尊重其基本权利和自由，尤其是个人数据保护的权利。本条例旨在促进实现一个自由、安全与公正的空间与经济联盟，推动经济和社会进步，促进内部市场经济的壮大和融合，增进自然人的福祉。
>
> 来源：《通用数据保护条例》(EU)2016 / 679；鉴于条款(2)

联系 EXIN

www.exin.com