《欧盟数据保护通用条例》详解

王融
中国信息通信研究院互联网法律中心，北京 100191

摘要
《欧盟数据保护通用条例》于 2018年 5月 25日正式生效。为踏上数字时代新秩序的起跑线，全球企业都在积极准备合规工作。全面梳理其带来的重大变化，既为企业提供参考，也为我国政府考虑大数据背景下的数据保护规则提供新视角。

关键词
数据保护通用条例；变化；合规

中图分类号：D93 文献标识码：A doi: 10.11959/j.issn.2096-0271.2016045

Deconstructing the EU General Data Protection Regulation

WANG Rong
Internet Law Center of China Academy of Information and Communication Technology, Beijing 100191, China

Abstract
The EU General Data Protection Regulation (GDPR) has taken effect on May 25, 2018. In order to catch up with the new trend of digital era, companies from all over the world are actively preparing for the related compliance work. The major changes of this new regulation were demonstrated comprehensively. It will provide a reference for companies and new prospective for China's data protection policy making in big data era.

Key words
General Data Protection Regulation (GDPR), change, compliance

1 引言

2012年，欧盟启动对1995年《数据保护指令》[①]（以下简称《指令》）的修订工作。在历经4年多的立法协商之后，《欧盟数据保护通用条例》（General Data Protection Regulation，GDPR）[②]（以下简称《条例》）已正式通过，并将于2018年5月25日全面实施。以下详细介绍《条例》带来的10个方面的主要变化。

2 变化1: 适用范围极大扩展

法律的适用范围从过去的属地主义向属人主义扩展。1995年的《指令》的适用范围取决于属地因素，要么机构的成立地在欧盟，要么利用欧盟境内的设备进行个人数据的处理活动（仅仅是传输通道除外）。新《条例》不仅考虑属地因素，还增加了属人因素。简言之如下。

- 对于成立地在欧盟的机构来说，法律的适用范围并没有发生大的变化，但强调了无论数据处理的活动是否发生在欧盟境内，都统一遵循《条例》。
- 对于成立地在欧盟以外的机构来说，则适用属人因素。只要其在提供产品或者服务的过程中（不论是否收费）处理了欧盟境内个体的个人数据，将同样适用于《条例》。此类情形还包括对欧盟境内个人活动的监控行为。根据《条例》说明部分的解释，监控行为包括了利用cookie等互联网技术工具对个人网络活动的跟踪分析（第3条）。

也就是说任何网站甚至App只要能够被欧盟境内的个人访问和使用、产品或服务使用的语言是英语或者特定的欧盟成员国语言、产品标识的价格为欧元，都可以被理解为该产品、服务的目标用户包括欧盟境内用户，从而需要适用《条例》。这也是缘何《条例》在全球引起极大震动的核心原因之一。不论是银行、保险、航空等传统行业，还是电子商务、社交网络等新兴领域，只要涉及向欧盟境内个人提供服务并处理个人数据，都将落入《条例》适用范围，除非放弃欧盟5亿发达人口市场。

3 变化2: 统一的法律规则之下仍有一些例外

此次立法主旨之一是结束1995年《指令》以来各成员国之间的数据保护法律制度差异问题，《条例》的统一规定将直接适用于各成员国。但值得注意的是，《条例》仍然为各成员国预留了一定自主空间，如下所示。

- 《条例》对于儿童个人数据做出了特殊保护规定，但允许成员国对于儿童的年龄标准在13~16岁做出调整（第8条）。
- 在处罚方面，《条例》规定了实施行政罚款的一般性条件，但同时也授权成员国规定其他处罚类型的规则，这些处罚适用于违反了《条例》但并不符合行政罚款条件的违法行为（第84条）。
- DPO（data protection officer，数据保护官）的设立。除了《条例》规定的必须设立DPO的情形，《条例》还授权成员国可以扩展必须设立DPO的其他情形（第37条）。
- 成员国可以在未来针对基因、生物识别以及健康数据的保护做进一步规定（第9条）。
- 成员国可以依据《条例》的基本原则，针对雇佣领域的数据保护，做出进一步的规定（第88条）。

除以上列举之外，在《条例》中此类授权成员国可作出进一步具体规定的条款还有很多。因此，尽管统一的《条例》为企业

① Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

② REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) THE EUROPEAN, 4.5.2016 L 119/1 Official Journal of the European Union

大大降低了合规的复杂性，但仍需注意到统一之外的差异性[③]。

4 变化3: 一站式监管

对于向欧盟不同国家提供业务的企业或者在不同国家都有设立地的企业来说，新《条例》会极大减轻合规成本。企业不再需要与多个不同成员国的数据监管机构打交道。根据新的一站式监管机制（one stop shop），企业主成立地所在国家的监管机构将作为主导监管机构（lead supervisory authority），对企业的所有数据活动负有监管权力，其效力辐射全欧。

当然，为保证监管的协调统一性，《条例》为此精心设计了一套复杂的咨询机制。主导监管机构的监管决定要最大程度上反映其他成员国监管机构的意见。如果不能达成一致意见，则交由欧盟数据保护委员会（European Data Protection Board，EDPB）处理（第56、60、61条等）。

5 变化4: 处理数据须有合法理由

处理个人数据必须要有合法理由，包括：数据主体的同意、履行合同需要、履行法定义务的需要以及数据控制者的合法利益等。以下对数据主体的同意、数据控制者的合法利益以及敏感数据的处理等重点条款作进一步的解释。

（1）关于数据主体的同意

《条例》对于数据主体的同意的有效标准相比《指令》严格很多。“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（第7条）。

在这种高标准下，虽然《条例》并没有明确禁止“推定同意”模式（敏感数据处理、数据画像活动除外），但在实践中通过推定方式获得用户同意将很难被认为是有效合法的。也就是说，当前实践中普遍存在的通过冗长晦涩的隐私政策来获取用户同意，或者让用户在签订业务协议时通过“打钩”方式作出一揽子授权的方式将失去合法性。业界普遍认为，《条例》关于有效合法同意的严格规定，使得用户的同意不会像现在这样被轻易获得[④]。

更重要的是，《条例》赋予了数据主体可以随时撤回同意的权利。数据控制者应当明确告知用户现有该权利，并为用户方便地行使该权利提供便利。

在处理儿童个人数据时，必须获得其父母或者其他监护人的同意。并且该举证责任在于数据控制者，数据控制者必须能够证明其从监护人那里获得了“同意”（第8条）。

（2）关于数据控制者的合法利益

1995年版的《指令》和《条例》都规定了除了获得“同意”以外的其他数据处理的合法理由。其中包括符合数据控制者的合法利益。一般认为，数据控制者出于营销目的对个人数据的使用要符合个人的合法利益，但同时《条例》赋予了数据主体对于营销活动的绝对反对权。换言之，数据控制者可以以营销为目的使用用户个人数据，但用户随时可以提出反对，数据控制者必须立即停止使用。除此之外，将数据控制者的合法利益作为数据处理的合法理由的情形在实践中非常有限。数据控制者必须能够证明，其合法的利益显著高于数据主体的个人权利和自由（第6条）。

③ http://www.gtlaw.com/News-Events/Publications/Alerts/194155/EU-General-Data-Protection-Regulation-What-Impact-for-Businesses-Established-Outside-the-EU

④ http://www.hoganlovells.com/en/publications/futureproofing-privacy-a-guide-to-preparing-for-the-eu-data-protection-regulation

（3）关于敏感数据的处理

敏感的个人数据包括：能够揭示个人的种族、政治倾向、宗教和哲学信仰、商业团体资格以及关于个人健康或者性生活的数据，在敏感数据类型中，《条例》还明确加入了基因数据和生物数据，这类数据的处理能够唯一地识别出特定个人（第9条）。

敏感个人数据的特殊性在于，作为一般法则，禁止处理敏感数据，除非特定的例外条件能够满足。这些例外条件包括：数据主体的同意，或者数据主体已经将上述信息公开；为了建立、履行或者保护合法的诉求必须处理上述敏感信息；为了公共利益的需要或者与公共利益相关的归档、科学、历史或者统计。但总体的原则是，这些对于敏感数据处理的例外情况的解释将会非常狭窄。

6 变化5：坚实强大的数据主体权利

相比于1995年版《指令》，《条例》对数据主体的权利规定细致入微，为个人有效行使权利提供了坚实的法律保障。

（1）知情权

《条例》规定数据控制者必须以清楚、简单、明了的方式向个人说明其个人数据是如何被收集处理的。可以想见的是，当前企业普遍应用的隐私政策必须进行大幅改革，才能满足合规要求。《条例》规定了应当告知用户的信息包括以下内容（第12、13条）。

- 数据控制者的身份和联系方式、数据控制者指定的代表信息、DPO的相关信息、数据的接收者或数据接收者的类型。
- 数据处理的目的和合法基础。如果合法基础是用户的“同意”，则要告知用户享有撤回“同意”的权利，并且该撤回不得影响先前的数据处理中用户的合法利益。该信息应当以单独、显著方式显示。
- 如果涉及自动化的数据处理，包括数据画像活动，则需要提供基本的算法逻辑以及针对个人的运算结果。
- 个人数据的保留周期以及采取该周期的理由。
- 依据法律，数据主体享有权利、投诉权以及相关的监管机构。
- 如果数据传输到第三国，则需要告知用户该第三国是否通过欧盟的充分性决定，如果没有通过，则需要告知数据控制者采取了何种保障措施。
- 如果数据不是从数据主体处直接收集而来，则需要告知其数据的来源和类型。

（2）访问权

数据控制者应当为用户实现该权利提供相应的流程，如果该请求是以电子形式提出的，则也应当以电子形式将数据提供给个人。控制者不能基于提供该服务而收费，除非数据主体的请求明显过量，超过负担（第15条）。

（3）反对权

对于两种情形，数据主体享有绝对的拒绝权：始终有权随时拒绝数据控制者基于其合法利益处理个人数据；始终有权拒绝基于个人数据的市场营销行为。《条例》还引入了限制处理的权利。例如，当数据主体提出投诉（如针对数据的准确性）时，数据主体并不要求删除该数据，但可以限制数据控制者不再对该数据继续处理（第21条）。

除了以上权利之外，《条例》还全面引入了新型的权利类型，其中最引入注目的是“数据可携权”（第20条）、“被遗忘权”（第17条）。

“个人数据可携权”，是指用户可以无障碍地将其个人数据从一个信息服务提供者处转移至另一个信息服务提供者。例如，Facebook的用户可以将其账号中的照片以及其他资料转移至其他社交网络服务提供商。当然，该权利不仅适用于社交网络服

务，还包括云计算、网络服务以及手机应用等自动数据处理系统。信息控制者不仅无权干涉信息主体的此项权利，还需要配合用户提供数据文本。从目前第20条规定来看，数据可携权适用于数据主体提供给数据控制者的数据，因此个人的网络行为轨迹是否属于该范畴，还有待于欧盟数据保护委员会做出解释。

“被遗忘权”，《条例》第17条删除权（“被遗忘权”）共计3款。其中，第1款的核心仍然是传统个人信息保护法中已经确立的删除权：当用户依法撤回同意或者数据控制者不再有合法理由继续处理数据时，用户有权要求删除数据。关于“被遗忘”的精神更多体现在第17条第2款：如果数据控制者将符合第1款条件的个人数据进行了公开传播，应该采取所有合理的方式予以删除（包括采取可用的技术手段和投入合理成本），数据控制者有责任通知处理此数据的其他数据控制者，删除关于数据主体主张的个人数据链接、复制件。也就是说，数据控制者不仅要删除自己所控制的数据，还要求数据控制者负责对其公开传播的数据，要通知其他第三方停止利用并删除。这是对传统“删除权”的扩张。

总体看来，《条例》对于数据主体权利的补充完善，不仅极大增强了数据主体对于个人数据的控制能力，也对企业如何保障实现数据主体的权利提出了具体的要求，对企业的制度建设、措施配置、业务流程乃至IT系统设计产生直接影响。

7 变化6：严格问责——数据控制者

《条例》大大简化了企业日常的合规负担，特别是废除了目前各成员国关于数据处理及境外转移的许可或者备案程序。但是取而代之的是要求企业在内部建立完善的问责机制，以实现《条例》规定的真正落地[5]。特别是，《条例》旨在对个人数据处理中的个人权利和自由提供充分的尊重和保障，因此，对于数据控制者和处理者的约束规范十分严格。欧盟数据保护机构第29条工作组已经将制定相关细则列为了工作优先项[6]。

7.1 DPO

对于设立地在欧盟的机构来说，以下是必须设立DPO的法定情形：

- 政府部门及公共机构作为数据控制者的；
- 机构核心业务涉及以下大规模活动：日常地以及系统性地监控数据主体、处理特殊类型的个人数据，或者数据处理活动与刑事定罪相关。

DPO必须具备数据保护专业知识和技能，有能力且能独立地履行职责。DPO的联系方式必须予以公布，且向监管机构报备。集团公司可以指定一位DPO，但前提是DPO能够方便地介入公司其他运营地，处理相关事务。此外需要注意的是，《条例》允许成员国通过国内立法扩展必须指定DPO的其他情形（第37条）。

对适用于《条例》，但设立地在国外的机构而言，其必须在欧盟境内指定一个代表（机构）[7]，以作为该机构与数据保护监管机构之间的联系点（第27条）。

7.2 文档化管理

文档化管理（documentation）的目的是做到一举一动都有据可查。数据控制者必须全面记载其数据处理活动，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、数据保存的时间、采取的安全保障措施等，保留与数据处理者的合同附件。

⑤ 需要说明的是，尽管1995年版《指令》中提出了数据控制者、数据处理者两个主体概念，但绝大部分法律要求是面向数据控制者提出的。新的《条例》继承了这两个主体概念，但是将数据处理者也直接纳入了规范的范畴。因此，本部分中关于数据控制者的问责机制同样适用于数据处理者。另，按照新《条例》，控制者是指单独或联合其他方决定了数据处理目的和方法的主体，包括自然人、法人，公共机构等，机构或者其他实体。处理者是指代表数据控制者进行数据处理的主体，包括自然人、法人、公共机构等机构或者其他实体（第4(7)、4(8)条）

⑥ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf

⑦ 代表可以是机构，也可以是个人，但应当具有处理个人数据保护事宜的专业能力

250人雇员以下的中小企业可以豁免该要求，但是核心业务涉及大规模的处理个人数据或者敏感数据以及涉及违法定罪数据处理的不能例外。文档化管理不仅是企业内部的管理措施，而且是数据保护监管机构履行职责的重要抓手（第30条）。

7.3 数据保护影响评估

对于高风险的数据处理活动，要事先进行数据保护影响评估（data protection impact assessment，DPIA）。《条例》并没有对高风险进行界定，但以下情形，应当事前评估：对个人特征的系统性评价（该评价会对数据主体产生法律上的影响）、对大量敏感数据的处理以及对公共领域大规模的系统性监控（第35条）。

7.4 事先协商

如果数据保护影响评估的结果显示是高风险，且数据控制者没有有效降低风险的措施，数据控制者应当就数据处理活动向相关的数据保护监管机构进行事先协商（prior consultation）。监管机构应当在收到协商申请的特定期限内提出处理意见，并可以采取纠正措施。除此之外，成员国在制定涉及数据保护的立法时，也应当事前征求数据保护监管机构的意见（第36条）。

7.5 数据泄露报告

《条例》将数据泄露定义为导致偶然的或者非法的数据破坏、损失、改变、非授权的披露等（第4（12）条）。一旦发生数据泄露事故，数据控制者需要及时通知监管机构，如果可行，应不超过72 h，除非该泄露不可能造成对个人权利和自由的破坏，若未在72 h内报告监管机构，则后续报告应当说明延迟报告的理由。对于数据处理者而言，其应当在意识到泄露事故及风险后及时报告数据控制者（第33条）。

数据泄露报告（data breach notification，DBN）中至少应当包含以下内容：关于数据泄露事故的描述，涉及的数据主体的总量、类型以及数据记录的总量，企业DPO的姓名和联系方式，泄露可能造成的结果，企业已经采取的止损措施。数据控制者应当将所有的数据泄露事故予以文档化，以便监管机构能够检查其合规工作（第33条）。

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（如加密）使得数据难以被一般人理解，或者其后续采取的措施能够使威胁不会成为实际的结果，则数据控制者可以不必履行数据泄露报告义务，但这些证明责任都在数据控制者。当然，数据监管机构可以否决数据控制者做出的风险判断，强制要求做出报告（第34条）。

依照《条例》规定，强制性的数据泄露报告是没有门槛的，因此企业应当为此建立周密的制度安排，包括数据安全管理流程、泄露事故发现、上报预案等，以符合条例的严格要求。

7.6 安全保障措施

《条例》对于安全保障（security of processing）措施给予了更具体的规定，特别强调了以下措施：

- 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（第32条）。

关于其中对于个人数据匿名和假名，

《条例》明显做出了区分。假名数据是指在缺乏其他信息的前提下(且该信息被独立存储),不能够被识别指向特定个人的数据。假名数据仍然属于个人数据,因此适用于个人数据的安全保障,特别是对于能够将假名数据恢复身份识别属性的额外信息必须单独安全存储。但相比于普通个人数据,假名数据在遵循的规范方面要相对宽松。例如假名化以后,数据控制者可以将数据用于收集该数据时所确定目的之外的其他目的。

匿名数据是指已经完全移除了个人可识别信息之后的数据,该数据不能够再识别出特定个人。匿名数据不再属于个人数据,不受《条例》规范。

8 变化7: 严格问责——数据处理者

对于数据处理者而言,《条例》带来了重大变化。1995年版《指令》主要适用于数据控制者。数据处理者主要通过合同的方式承担数据保护责任。然而新《条例》对于数据控制者、数据处理者在大多数情况下提出了相同的要求,例如数据处理者也承担对数据的安全保障义务,在管理措施、技术上采取必要的措施,包括指定DPO、在发生数据泄露事故时及时报告数据控制者等。

此外,《条例》还细致规定了数据控制者和数据处理者之间的合同应当至少包含哪些内容,例如数据处理的目的、期限、个人数据的类型、数据主体的类别以及双方的权利业务。

数据处理者仅能按照数据控制者书面的要求处理数据,必须确保其员工能够遵守有关保密的要求;在数据安全、数据泄露、数据保护影响评估等方面对数据控制者提供协助。如果没有数据控制者的同意,数据处理者不得二次分包业务;数据控制者可以对分包采取概括性授权,但如果具体的分包商发生了变化,数据处理者有义务及时告知数据控制者,后者有权提出反对。数据处理者对其分包商的数据处理活动完全负责,有义务将数据保护的要求施加给二级分包商。在数据处理服务终止时,数据处理者应当删除或者将数据全部返还给数据控制者,除非根据法律的要求必须保留这些数据。

数据处理者的违规行为同样将受到《条例》规定的严格处罚,数据监管机构扩展的监管权力也同时适用于数据处理者,包括进入数据控制者的工作场所、发布警告、发布数据处理禁令等。用户个人也有权直接从数据处理者处主张赔偿,当然如果是因为数据控制者的错误指令,则数据处理者可以再向数据控制者索赔(第28条)。

新规中对数据处理者构建的一系列规范要求,将对当前的云计算生态体系带来重大影响。按照新规,数据控制者和数据处理者之间的合同在很多情形下需要重新谈判达成。特别是由于《条例》使数据处理者大大增加了合规风险,二者合同中关于安全保障措施、风险管理以及服务的价格都会受到影响。

9 变化8: 完善跨境数据流动机制

关于跨境数据流动的限制是在1995年版《指令》中提出的,欧盟公民的个人数据仅能转移到与欧盟同等保护水平的国家。在实践中,部分成员国针对跨境数据流动增加了事前的备案或者许可要求。新《条例》明确禁止了这种增设许可的做法,只要符合《条例》中跨境数据流动的条件,则成员国不得再予以限制。在此基础上,《条例》还进一步完善了数据转移合法机制。

(1)充分性决定

相比于1995年版《指令》,欧盟委员会除了可以对国家作出评估外,还可以对一国内的特定地区、行业领域以及国际组织的

保护水平作出评估判断。这进一步增加了通过“充分性”决定(adequate decision)的灵活性。毕竟自1995年版《指令》实施以来,通过充分性决定的国家及地区还不超过10个[⑧]。《条例》对欧盟委员会做出充分性决定的程序和标准也进行了进一步详细规范,包括要求至少每隔4年对充分性决定进行重新审查(第45条)。

(2)有约束的公司规则

有约束的公司规则(binding corporate rules, BCR)最早由欧盟第29条工作组发展而来,初衷是让跨国公司或者公司集团能够在公司内部进行跨境的数据转移,是欧盟委员会提出的标准化格式合同的一个替代选择。在1995年版《指令》框架下,大约有2/3的欧盟成员国认可BCR。但是取得成员国监管机构对于BCR的认可需要经历冗长的批准程序(18~24个月不等)。此次《条例》对BCR给予了正式的法律地位,并详细规定了BCR获得认可的程序和内容标准(第47条)。

(3)标准合同条款

目前欧盟委员会通过的3个标准合同条款(standard contractual clauses)仍然有效。《条例》增加了成员国数据监管机构可以指定标准合同条款的渠道,但必须要经过欧盟委员会的认可(第63条)。

(4)经批准的行为准则

数据控制者可以成立协会并提出遵守《条例》的详细行为准则(codes of conduct)。该行为准则可以由成员国监管机构或者欧盟数据保护委员会批准,并通过有约束力的承诺方式生效。这种情形主要针对不适用于《条例》但从欧盟接收数据的主体(第46条)。

(5)经批准的认证机制、封印或者标识

经批准的认证机制、封印或者标识(approved certification mechanism,seal or mark)主要适用于公共机构之间的数据转移活动。行为准则与认证机制是《条例》中引入的新型合规机制,以最大化发挥第三方监督与市场自律作用。

10 变化9:对数据画像活动的特别规制

根据《条例》界定,“数据画像”(profiling)概念外延广泛,它是指:任何通过自动化方式处理个人数据的活动,该活动服务于评估个人的特定方面,或者专门分析及预测个人的特定方面,包括工作表现、经济状况、位置、健康状况、个人偏好、可信赖度或者行为表现等。这一概念被普遍认为能够覆盖目前大多数利用个人数据的大数据分析活动,如对个人偏好的分析,可涵盖市场中最普遍的大数据分析市场营销活动。

画像活动如果对用户个人产生法律上的影响或者其他重大影响,仅仅在符合以下条件之一时才是合法的:①数据主体明确同意;②欧盟或者成员国法的明确授权;③数据主体和数据控制者之间签订、执行合同所必需(第22条)。考虑到②③仅仅是个别情形,因此,实践中绝大部分的数据画像的合法基础是用户明确同意。而根据《条例》对于“同意”的高标准要求,业内专家认为,获得用户在数据画像方面的同意将是难以操作的,这将对大数据背景下的分析营销活动带来极大的负面影响[⑨]。

在数据画像活动中,获得用户合法有效的同意,首先应当向数据主体全面介绍数据画像处理活动是怎么进行的,收集了用户的哪些数据,算法的基本原理是什么,评估结果是否会对用户产生法律上的影响。其次,应当明确告知用户其享有对画像的反对权。此类信息应当明确无误地表达,并使用足够引起用户注意的范式,独立于其他信息(第13.2、21条)。

此外,基于个人敏感数据的数据画像

⑧ 加拿大于2002年、阿根廷于2003年、瑞士于2004年、安道尔共和国于2010年、以色列于2011年、新西兰于2013年、英国马恩岛于2004年、美国新泽西州于2008年、丹麦法罗群岛于2010年通过充分性决定

⑨ https://www.huntonprivacyblog.com/2016/04/12/hunton-releases-2016-eu-general-data-protection-regulation-guide-for-in-house-lawyers/

活动是被禁止的，除非数据主体出于一个或者多个特定的目的，被给予了明确的同意，但是成员国可以通过立法明确规定即使在用户同意的情况下，也禁止基于敏感数据的画像活动；或者该数据画像活动对于重大的公共利益是必需的（第22条）。

因此，对于依赖于数据画像（包括利用cookie等跟踪工具开展行为精准营销）的企业来说，如何设计一套有效的机制，既能够符合《条例》有关透明性和用户同意的要求，同时也能使得数据分析活动得以继续，是当前的一道难题。

11 变化10：监管权力、处罚与司法救济

《条例》增强了监管机构的执法权，包括：通知数据控制者、处理者相关违反行为；要求违法者提供相关信息，或者向监管机构提供访问此类信息的接口；现场调查、审计；命令修改、删除或者销毁个人数据；可以采取临时性的或者限定性的数据处理禁令；科以罚金（第58条）。

《条例》规定了严苛的罚金，分为两档：①处以1 000万欧元或者上一年度全球营收的2%的罚款，两者取其高。针对的违法行为包括：没有实施充分的IT安全保障措施，或者没有提供全面的透明的隐私政策，没有签订书面的、数据处理协议等；②处以2 000万欧元或者企业上一年度全球营业收入的4%的罚款，两者取其高。此类处罚针对的违法行为包括：无法说明如何获得用户的同意，违反数据处理的一般性原则，侵害数据主体的合法权利以及拒绝服从监管机构的执法命令等（第83条）。

司法救济。对于不服监管机构作出的决定或者针对监管机构的不作为，当事主体可寻求司法救济。其中，数据主体可以通过司法途径向数据控制者、数据处理者主张因其违反《条例》而致使数据主体遭受物质上或者非物质上的损害。如果一个以上的数据控制者、处理者涉及侵权，则共同承担连带责任，除非其能证明对损害的产生没有责任。上述司法救济的权利可以由消费者机构代表数据主体行使（第26、80、82条）。

12 结束语

从1995年版《指令》的34个简单条文扩展到99条（263页）的详细规范，《条例》带来了全面制度改革，其核心目标是将个人数据保护深度嵌入组织运营，真正将抽象的保护理论转化为实实在在的行为实践。对于企业而言，小至隐私政策、业务流程，大到IT系统、战略布局，无一不需要重新审视规划。当下着手的准备工作，决定了企业能否有底气在2年之后站立在数字时代新的起跑线上。

作者简介

王融（1979-），女，中国信息通信研究院互联网法律中心副主任、高级工程师，主要从事电信、互联网立法与监管政策研究工作。代表著作：《电信法》《融合背景下的中欧电信管制比较研究》《个人信息保护法研究》。主要研究方向为个人信息保护法、网络信息安全法。发表文章30余篇。负责及参与中央网络安全和信息化领导小组办公室、工业与信息化部、中欧信息社会等委托研究项目，参与国家《电子商务法》《网络安全法》及工业和信息化部部门规章立法工作。

收稿日期：2016-06-20