欧盟 《一般数据保护条例》

来源：公众号“数据法律资讯”（ID：DATA_AND_LAW；Email：dataprotection@163.com）
翻译：洪东荧(1—16)、李立（17—32）、余超（33—54）、孙磊（55—74）、施佳倩（75—87）、孟庆海（88—99）
校对：高富平 王文祥 施佳倩
文档制作：公众号“顶象业务安全”（ID：dingxiang-tech）

立法进程

2012 年 1 月 25 日，欧盟委员会发布建议修订的数据保护框架，即 2012 年草案（见本书）。
2014 年 3 月 12 日，欧盟议会采纳了许多有关于 2012 年草案文本的修订意见，形成欧盟议会稿（未译出）。
2015 年 12 月 17 日，欧盟常住代表委员会(Committee of Permanent Representatives)签署了条例文本，结束了欧盟议会、欧盟理事会和欧盟委员会三个机构的磋商。
2016 年 1 月 5 日，欧盟议会非正式地批准条例(48 票赞成，4 票反对，4 票弃权)。
2016 年 4 月 14 日，欧盟议会正式批准了《统一数据保护条例》，使该条例成为欧盟的立法。欧盟成员国有 2 年的过渡期，以适用该条例来取代原来的国内立法。条例正式于 2018 年生效。

第一章 一般性规定

第一条 主体和目标

1.本条例旨在确立个人数据处理中的自然人保护和个人数据自由流通的规范。

2.本条例旨在保护自然人的基本权利和自由，尤其是个人数据保护的权利。

3.个人数据在欧盟境内的自由流通不得因为在个人数据处理过程中保护自然人而被限制和禁止。

第二条 适用范围

1.本条例适用于全部或部分通过自动化手段进行的个人数据处理行为，以及通过自动化手段以外的其他方式进行的、构成或旨在构成存档系统一部分的数据处理行为。

2.以下个人数据处理的情形不适用本条例的规定：

(a)在欧盟法律管辖范围外的活动；

(b)成员国实施《欧洲联盟条约》(Treaty on European Union)第五编第二章范围内的活动；

(c)自然人实施的纯粹个人或家庭活动；

(d)有权机关为预防、调查、侦查、起诉刑事犯罪或执行刑罚的目的所进行的数据处理，其中包括预防与抵御公共安全风险。

3.《对欧盟机构和团体进行的个人数据处理中涉及的个人保护与数据自由流通条例》[Regulation（EC）No 45/2001]适用于欧盟机构、团体、办事处和代理机构所实施的数据处理行为。《对欧盟机构和团体进行的个人数据处理中涉及的个人保护与数据自由流通条例》[Regulation(EC)No 45/2001]以及其他可适用于个人数据处理的欧盟法令应当依照本条例第98 条的规定作出调整以适用本条例的原则和规则。

4.本条例不影响《电子商务指令》(2000/31/EC)的实施，特别是对该指令第 12 至 15 条关于中介服务提供者法律责任规定的实施。

第三条　地域管辖范围

1.本条例适用于营业场所(establishment)设在欧盟境内的数据控制者和处理者所进行的个人数据处理活动，而不论该处理行为是否发生在欧盟境内。

2.当数据处理活动涉及以下情形时，本条例适用于非设立于欧盟境内的数据控制者或处理者对位于欧盟境内的数据主体的个人数据所进行的数据处理行为

(a)为欧盟境内的数据主体提供货物或服务，而不论数据主体是否被要求付费；

(b)对数据主体在欧盟境内的行为进行监控。

3.本条例适用于非设立于欧盟境内但根据国际公法的规定适用成员国法律的数据控制者所进行的个人数据处理行为。

第四条　定义

在本条例中：

(1)个人数据(personal data)：是指与已识别或者可识别的自然人（数据主体）相关的任何数据；可识别的自然人尤其是指通过姓名、身份证号、定位数据、网络标识符号以及特定的身体、心理、基因、精神状态、经济、文化、社会身份等识别符能够被直接或间接识别到身份的自然人；

(2)数据处理(processing)：是指对个人数据进行的任何操作或者一系列 操作，无论其是否通过自动化手段进行，如数据收集、记录、组织、建构 (structuring)、存储、改编或修改，恢

复、查询、使用、通过传播、分发 (dissemination)方式进行披露或者其他使个人数据可被他人获得、排列或组合、限制、清除或销毁(destruction)的操作;

(3)处理限制(restriction of processing):是指为了限制数据在将来的处理而对所存储的个人数据予以标记;

(4)识别分析(profiling):是指对个人数据采取的任何自动化处理的方式,包括评估某个自然人特定方面的情况,尤其是为了分析和预测该自然人的工作表现、经济状况、健康、个人喜好、兴趣、可信度、行为举止、所在位置或行迹;

(5)假名化机制(pseudonymisation):是指以如下方式处理个人数据,即:除非使用额外信息,否则无法将个人数据连结到某个具体的数据主体,且上述额外信息应当被独立存储并受制于适当的技术和组织措施,以确保个人数据不会连结到某个已识别或可识别的自然人;

(6)数据存档系统(filing system):是指依据特定标准可进行访问的结构化的个人数据集合体,无论它们在功能上或在地理上是集中的、非集中的还是完全分散的;

(7)数据控制者(controller):是指单独或与他人共同确定个人数据处理的目的和方式的自然人、法人、公共权力机关、代理机构或其他机构;这里个人数据处理的目的和方式应由欧盟或成员国法律决定,数据控制者或其任命的具体标准也可由欧盟或成员国法律规定;

(8)数据处理者(processor):是指代表数据控制者处理个人数据的自然人、法人、公共权力机关、代理机构或其他机构;

(9)数据接收者(recipient):是指作为个人数据的披露对象的自然人、法人、公共权力机关、代理机构或其他机构,而不论其是否为第三方主体;但依据欧盟或成员国法律在特定调查范围内实施数据接收行为的公共权力机关不被视为数据接收者;公共权力机关对该部分数据的处理行为应当根据该处理行为的目的遵循可适用的数据保护规则;

(10)第三方(third party):指数据主体、数据控制者、数据处理者以及根据数据控制者或数据处理者的直接授权而处理数据的人之外的任何自然人或法人、公共权力机关、代理机构或其他机构;

(11)数据主体的同意(consent of the data subject):是指数据主体依据其个人意愿,自由、明确、知情并清楚地通过陈述或积极行为表示对其个人数据进行处理的同意;

(12)个人数据泄露(personal data breach):是指破坏数据的安保措施导致转移中的、存储的或其他处理中的个人数据被意外或非法的销毁、丢失、修改、未经授权的披露或访问;

(13)基因数据(genetic data):是指自然人先天继承和后天获得的有关基因特征的数据;该数据可以提供该自然人独特的生理或健康信息,该信息尤其可以通过对该自然人的生物样本进行分析而得;

(14)生物特征数据(biometric data):是指通过对自然人的身体、生理或行为特征进行特定技

术处理而得的个人数据，并能够识别自然人的身份，诸如面部图像或指纹数据(dactyloscopic data)；

(15)健康数据(data concerning health)：是指与个人身体和心理健康相关的数据，包括显示自然人健康状况的医疗保健服务中的信息；

(16)主要营业场所(main establishment)：

(a)对于数据控制者在多个成员国内设有营业场所的，将其位于欧盟境内的管理中心视为主要营业场所。但是如果对于个人数据处理的目的和方式的决策是由数据控制者位于欧盟境内的另一营业场所作出，且该营业场所具有执行上述决策的权力时，将做出这类决策的营业场所视为主要营业场所；

(b)数据处理者在多个成员国内设有营业场所的，将其位于欧盟境内的管理中心视为主要营业场所；如果数据处理者在欧盟境内没有管理中心，则将其在欧盟境内以受本条例具体义务约束的处理活动为主要活动的营业场所视为其主要营业场所。

(17)代表人(representative)：是指由数据控制者或数据处理者依照第 27 条的规定书面指定的，代表数据控制者或数据处理者履行本条例义务的，设立于欧盟境内的自然人或法人；

(18)企业(enterprise)：是指以任何组织形式从事经济活动的自然人或法人，包括持续从事经济活动的合伙企业或协会；

(19)企业集团(group of undertakings)：是指居于控制地位的控制公司和被其控制的公司；

(20)公司约束规则(binding coperate rules)：是指为规范某一联合经济活动中的企业集团向一个或多个第三方国家的数据控制者或处理者进行一次或一系列的个人数据转移活动，在某一成员国境内设立的数据控制者或处理者所要遵守的个人数据保护政策；

(21)监管机构(supervisory authority)：是指成员国依据本条例第 51 条建立起的独立公共权力机构。

(22)有关监管机构(supervisory authority concerned)：是指因为以下情况而作为个人数据处理行为的监管机构：

(a)数据控制者或处理者设立于监管机构所在国的境内；

(b)居住于监管机构所在国境内的数据主体实质上已经或可能受到该数据处理的影响；

(c)已向该监管机构提出投诉；

(23)跨境处理(cross-border processing)是指以下任一情况：

(a)数据控制者或数据处理者在多个成员国境内多个营业场所所开展的数据处理营业活动；

或

(b)个人数据处理发生在位于欧盟境内的数据控制者或数据处理者的单一营业场所，但该活动实际上或可能会影响到多个成员国的数据主体。

(24)关联及合理的异议(relevant and reasoned objection)：是指对是否存在违反本条例的侵权行为提出异议，或在决议草案已经清楚说明会对数据主体的基本权利和自由甚至会对个人数据在欧盟境内的自由流通造成巨大风险时， 对数据控制者及数据处理者所计划的活动是否遵守本条例规定而提出异议。

(25)信息社会服务(information society service)：是指欧盟议会及理事会颁布的《制定关于技术规范信息和信息社会服务规制的提供程序的指令[Directive(EU)2015/1535]第 1 条第 1 款(b 项所定义的服务。

(26)国际组织(international organisation)：是指受国际公法调整的组织及其附属机构，或者是由两个或两个以上国家设立或建立在他们之间的协定基础之上的其他组织。

第二章　原则

第五条　个人数据处理的原则

1.个人数据的处理必须遵循以下原则:

(a)合法地、公平地并且以公开透明的方式对数据主体的个人数据进行处理（合法、公平和透明）;

(b)基于具体、明确、合法的目的收集个人数据，且随后不得以与该目的相违背的方式进行处理；第 89 条第 1 款中为实现公共利益存档目的、科学研究或历史研究目的、统计目的而进行的进一步数据处理不视为与最初目的相违背（目的限制）;

(c)数据应是充足的、相关的并且限于数据处理目的最小必要范围（最小范围原则）;

(d)数据应是准确的，且若有必要应保持适时更新，采取一切合理措施确保与数据处理目的相悖的错误数据被及时清除或更正（准确性原则）;

(e)以可识别数据主体身份的形式存储的数据的存储时间不能长于实现个人数据处理目的所必须的时间；个人数据仅在依据第 89 条第 1 款的规定，为公共利益存档目的、科学研究或历史研究目的、数据统计目的的情况下才可被储存更长时间，而且为保障数据主体的权利和自由，个人数据还应受本条例要求的适当技术和组织措施的调整（存储限制原则）;

(f)数据处理应当以确保个人数据的适当安全性的方式进行，包括采取适当的技术或组织措施以保护数据免遭未经授权或非法的处理以及意外的丢失、销毁或破坏（完整性和保密性）。

2.数据控制者应当对上述原则的落实情况承担责任并予以证明（责任原则）。

第六条　数据处理的合法性（Lawfulness of processing）

1.只有符合以下情况之一的个人数据处理行为才是合法的:

(a)数据主体已经对基于一个或多个具体目的而处理其个人数据的行为表示同意;

(b)履行数据主体为一方当事人的合同或在订立合同前为实施数据主体要求的行为所必要的数据处理;

(c)为履行数据控制者的法定义务所必要的数据处理;

(d)为保护数据主体或另一自然人的重大利益所必要的数据处理;

(e)为履行涉及公共利益的职责或实施已经授予数据控制者的职务权限所必要的数据处理;

(f)数据控制者或第三方为追求合法利益目的而进行的必要数据处理，但当该利益与要求对个人数据进行保护的数据主体的基本权利和自由相冲突时，尤其是当该数据主体为儿童时，则不得进行数据处理;

公共权力机构执行任务时实施的数据处理不受第 1 款（f）项的约束。

2.对符合本条第 1 款(c)项和(e)项规定的数据处理，成员国可以维持本条例的规则或者作出比本条例更加具体的规定，通过对处理行为设立更为精细的具体要求和其他措施来确保数据处理的合法与公平，其中包括第九章规定的其他具体处理情形。

3.依据本条第 1 款(c)项和(e)项进行的数据处理的基础必须出自以下法律:

(a)欧盟法律;

(b)数据控制者必须遵守的成员国法律。

考虑到本条第 1 款(e)项规定的处理行为，数据处理的目的应当在法律依据中予以确定或应当是为履行涉及公共利益的职责或实施已经授予数据控制者 的职务权限所必要的。该法律依据可以包含具体的条款来调整本条例的适用，尤其是：决定数据控制者处理行为合法性的一般条件；被处理的数据的类型；相关的数据主体；数据可能被披露的实体对象和披露目的；目的的限制；存储期限； 处理操作和处理程序，包括确保处理行为的公平与合法的措施，前述处理行为如本条例第九章规定的其他具体处理情形。欧盟或成员国法律应当实现公共利益的目标并且与立法所追求的合法利益目的相当。

4.当非基于数据收集的目的而进行的数据处理行为没有依据数据主体的同意或没有遵守作为民主社会中保障本条例第 23 条第 1 款的目标的必要且适当措施的欧盟或成员国法律时，为查明基于该述目的所进行的数据处理是否符合最初收集个人数据时的目的，数据控制

者尤其应当考虑以下情形:

(a)意图实施的后续处理行为的目的与收集个人数据时的目的之间的联系;

(b)个人数据被收集时的情形，尤其是关于数据主体与数据控制者之间的关系;

(c)个人数据的性质，尤其是所处理的个人数据是否属于本条例第 9 条所规定的特殊种类，或所处理的个人数据是否与本条例第 10 条规定的与刑事定罪与犯罪相关联;

(d)意图实施的后续处理行为会对数据主体造成的可能后果;

(e)存在适当的保障措施，其中可能包括加密措施或假名化机制。

第七条　同意的条件

1.当数据处理必须基于数据主体的同意时，数据控制者应当证明数据主体已经对处理其个人数据的行为予以同意。

2.如果数据主体是通过书面声明的方式表示同意的，而该声明还涉及其他事项，则同意在形式上应当满足：明显区分于其他事项，以明了且易获取的形式，　使用清楚简单的语言。该声明中任何与本条例规定相违背的内容不发生法律约束力。

3.数据主体有权在任何时候撤销其同意。该撤销不具有溯及力。在作出同意的意思表示之前，应将上述事项明确告知数据主体。撤销同意和作出同意应一样容易。

4.在评估时应当尽最大可能考虑数据主体的同意是否是基于自由意志作出，　尤其是在：包含服务条款的合同的履行是以数据主体同意其个人数据被处理为条件，而该数据处理又不为履行合同所必要。

第八条　信息社会服务中儿童同意的适用条件

1.在向儿童直接提供信息社会服务的情形中适用本条例第 6 条第 1 款(a)项的规定时，只有对年龄不小于 16 周岁的儿童的个人数据进行的处理行为才是合法的。对年龄不满 16 周岁的儿童，处理行为只有或至少在获取了该儿童的监护人的同意或授权时才是合法的。

成员国出于特定目的可以在法律上规定更加低的年龄界限，但是不得低于 13 周岁。

2.数据控制者应当考虑可利用的技术并作出合理的努力以核实在涉及儿童的情形中该儿童的监护人给予同意或授权的情况。

3.本条第 1 款的规定不得影响成员国一般合同法的适用，如涉及儿童的关于合同有效性、合同成立或合同效力的规定。

第九条　对特殊类型个人数据的处理

1.禁止在个人数据处理中泄露种族或民族起源、政治观点、宗教信仰、哲学信仰、工会成员资格等个人信息，禁止以识别自然人身份为目的对个人基因数据、生物特征数据的处理，禁止对健康数据、性生活、性取向等相关数据进行处理。

2.上述第 1 款的规定不适用于以下情况：

(a)数据主体明确同意数据控制者出于一个或多个特定目的对其个人数据进行处理，但按照欧盟或成员国法律的规定第 1 款的禁止性规定可能不取决于数据主体同意的除外；

(b)为就业、社会保险与社会保障法领域内的数据控制者或数据主体履行义务、实现特定权利的目的所必要的数据处理，该义务与权利来源于欧盟或成员国法律或者是根据为保障数据主体的基本权利与利益而提供了适当保护措施的成员国法律所起草的集体协议；

(c)当数据主体在生理上或法律上丧失同意的能力时，为保护数据主体或其他自然人的重大利益所必要的数据处理行为；

(d)基金、社团或其他非盈利机构出于政治、哲学、宗教或工会的目的，　在有适当的安全保障措施之下开展的合法活动中进行的数据处理行为，且该数据处理仅涉及到该机构的成员或前成员或基于机构的上述目的而与其保持经常性联系的人，且未经数据主体的同意个人数据没有对外披露；

(e)对数据主体已经明确公开的个人数据的数据处理行为；

(f)为提起诉讼、应诉或法院行使其司法权所必要的数据处理行为；

(g)欧盟或成员国法律应当与其立法目的相称，尊重数据保护权利的本质，规定适当且具体的措施以保障数据主体的基本权利与利益，基于这些法律，为实现实质的公共利益所需而进行的数据处理行为；

(h)基于欧盟或成员国法律的规定或是根据与保健医生签订的合同，且符合本条第 3 款规定的具体条件和保障措施，出于预防医学和职业医学的目的且为评估劳动者的工作能力、医疗诊断、提供健康、社会保障、治疗、健康管理或社会保障系统和服务所必要的数据处理行为；

(i)欧盟和成员国法律规定了适当且具体的措施以保障数据主体的基本权利和利益，尤其针对职业秘密。基于这些法律的规定，为实现公共卫生领域的公共利益所必要而进行的数据处理行为，诸如抗击严重的跨境卫生威胁，确保卫生保健、医疗产品、医疗设备的质量和安全的高标准；

(j)欧盟或成员国法律应当与其立法目的相称，尊重数据保护权利的本质，规定适当且具体的措施以保障数据主体的基本权利与利益，基于这些法律，依据本条例第 89 条第 1 款的规定，出于实现公共利益存档目的、科学研究或历史研究目的或统计的目的所必要的数据处理行为。

3.根据欧盟或成员国法律或成员国国内有权机关制定的规则应当承担专业保密义务的专业人士或其他人处理本条第 1 款规定的个人数据时，这些数据可以基于本条第 2 款(h)项的目的被处理。

4.对基因数据、生物特征数据或健康数据的处理，成员国可以维持或者引入更进一步的限制条件。

第十条　与刑事定罪和犯罪相关的个人数据的处理

根据本条例第 6 条第 1 款的规定对与刑事定罪和犯罪或保安处分相关的个人数据的处理，应当在官方机构的管理(control)之下或者是在规定了保障数据主体权利与自由的措施的欧盟或成员国法律的授权之下进行。任何对刑事定罪信息的全面登记都只能在官方机构的管理下进行。

第十一条　无需识别数据主体身份的数据处理(Processing which does not require identification)

1.如果数据控制者处理数据的目的不需要或不再需要识别数据主体的身份，　则不得强制数据控制者仅以遵守本条例的规定为由来保留、获取或处理额外信息以识别数据主体的身份。

2.在本条第 1 款规定的情况下，数据控制者能够证明自己不以识别数据主体身份为目的，如果数据控制者能够告知相应的数据主体，则其应当履行告知义务。在该情况下，不得适用本条例第 15 至 20 条的规定，除非数据主体为了行使其在这些规定中的权利而提供额外信息以使控制者能够识别其身份。

第三章　数据主体的权利

第一节 透明和形式

第十二条　信息与通信的透明以及数据主体行使权利的形式

1.数据控制者应当采取适当的措施将第 13 条和第 14 条规定的信息和第 15 至 22 条以及第 34 条规定的有关数据处理的通信通过清晰易懂的语言以一种简洁明了、透明以及易获得的形式提供给数据主体，尤其是专门针对儿童的信息，使用清楚的语言。这些信息应当以书面或者其他的方式提供，包括使用电子方式。在数据主体的身份可被其他方式证实时，若数据主体提出要求，控制者也可以通过口头方式提供信息。

2.数据控制者应当根据第 15 至 22 条的规定帮助数据主体行使其权利，在第 11 条第 2 款规定的情形中，控制者不得拒绝执行数据主体根据第 15 至 22 条规定行使其权利的要求，除非控制者证明其无法识别数据主体的身份。

3.对于数据主体根据第 15 条至 22 条的规定作出的请求，数据控制者不得无故拖延并且必

须在收到请求之日起一个月内提供其对这些请求所采取的应对措 施的信息。考虑到请求的数量和复杂性，在必要的时候上述期限可以延长两个月。控制者应当在收到请求之日起一个月内将上述延期情况连同延期的原因告知数 据主体。数据主体以电子方式提出请求的，数据控制者在可能的情况下也应以电子方式提供信息，除非数据主体有另外的要求。

4.如果数据控制者没有对数据主体的请求采取行动，其应当毫不延迟且至迟必须在收到请求的一个月内通知数据主体其没有采取行动的原因以及数据主体可以向监管机构投诉和寻求司法救济的可能性。

5.根据第 13 条和第 14 条提供的信息、通信以及根据第 15 至 22 条和第 34 条采取的行动都应当是免费的。数据主体的请求明显不合理或过分的，尤其是重复请求的，数据控制者也可以采取如下行为：

(a)考虑到提供信息、通信或采取数据主体所请求的措施所需要的行政花费，收取合理的费用；或者

(b)拒绝对数据主体的请求采取行动；

数据控制者应当承担证明请求明显不合理或过分的证明责任。

6.在不影响第 11 条的情况下，当数据控制者对于根据第 15 条至 21 条规定做出请求的自然人的身份有合理怀疑时，控制者可以请求数据主体提供额外的必要信息来确认数据主体的身份。

7.根据第 13 条和第 14 条提供给数据主体的信息可以结合标准化图标(icons) 的方式来提供，从而通过一个可视化、简洁明了且清晰易读的方式提供关于未来 处理行为的有意义的概述。以电子化方式呈现的图标应当是机器可读的。

8.根据本条例第 92 条的规定，授权欧盟委员会通过授权性法令(adopt delegated acts)来决定图标所呈现的信息和标准化图标的提供程序。

第二节 信息与个人数据的访问

第十三条 从数据主体处收集个人数据时（数据控制者）应提供的信息

1.从数据主体处收集与之相关的个人数据时，数据控制者应当在获取数据的同时向数据主体提供以下信息：

(a)数据控制者的身份信息和联系方式，以及数据控制者代表人（如果有）的身份信息和联系方式；

(b)数据保护专员（如果有）的身份信息和联系方式；

(c)处理个人数据的目的以及其合法基础；

(d)依据第 6 条第 1 款(f)项的规定处理数据时，数据控制者或第三方所追求的合法利益；

(e)个人数据的接收者或者接收者的类别(如果有)；

(f) 如果有，数据控制者意欲向第三国或国际组织转移数据的事实，以及欧盟委员会是否作出数据保护充分性决定的情况，或在本条例第 46 条或第 47 条或第 49 条第 1 款第 2 段规定的转移情形下获取个人数据或其副本的方式和相应的安全保障措施。

2.除了本条第 1 款规定的信息之外，数据控制者从数据主体获取个人数据时还应当进一步提供以下为确保处理行为公平、透明所必要的信息：

(a)个人数据的存储期限，若不可能，则应提供决定存储期限的标准；

(b)数据主体享有向数据控制者请求访问、更正、清除个人数据的权利， 限制、拒绝其处理个人数据的权利以及持续控制权；

(c)针对依据第 6 条第 1 款(a)项或第 9 条第 2 款(a)项的规定而进行的数据处理，数据主体有权随时撤销其同意，该撤销不具有溯及力；

(d)向监管机构投诉的权利 ；

(e)提供个人数据是出于法律要求、合同要求，还是为订立合同所必要的要求，数据主体是否必须提供个人数据，如不能提供，其可能的法律后果；

(f)本条例第 22 条第 1 款及第 4 款所规定的包括识别分析在内的自动化决策的存在，同时在这些情况下，至少提供关于决策中所运用的逻辑的有用信息以及该处理的重要性和其对数据主体造成的可能后果。

3.当数据控制者意图基于不同于数据收集初始目的的其他目的处理数据时， 数据控制者应当在进行进一步处理之前向数据主体提供有关新目的的信息以及 本条第 2 款所规定的所有相关信息。

第十四条　个人数据并非自数据主体处获得时（数据控制者）应提供的信息

1.当个人数据并非自数据主体处获得时，数据控制者应当向数据主体提供以下信息：

(a)数据控制者的身份信息和联系方式，以及数据控制者代表人（如果有） 的身份信息和联系方式；

(b)数据保护专员（如果有）的身份信息和联系方式；

(c)处理个人数据的目的以及其合法基础；

(d)相关个人数据的种类；

(e)个人数据的接收者或者接收者的类别（如果有）；

(f)如果有，数据控制者意欲向第三国或国际组织转移数据的事实，以及欧盟委员会是否作出数据保护充分性决定的情况，或在本条例第 46 条或第 47 条或第 49 条第 1 款第 2 段规定的转移情形下获取个人数据或其副本的方式和相应的安全保障措施。

2.除了本条第 1 款规定的信息之外，数据控制者还应当进一步提供以下为确保处理行为公平、透明所必要的信息：

(a)个人数据将被存储的期限，若不可能，则应提供决定存储期限的通常标准；

(b)依据第 6 条第 1 款(f)项的规定处理个人数据时，数据控制者或第三方所追求的合法利益；

(c)数据主体享有向数据控制者请求访问、更正、清除个人数据的权利， 限制、拒绝其处理个人数据的权利以及持续控制权；

(d)针对依据第 6 条第 1 款(a)项或第 9 条第 2 款(a)项的规定而进行的数据处理，数据主体有权随时撤销其同意，该撤销不具有溯及力；

(e)向监管机构投诉的权利；

(f)个人数据的来源，以及是否来自于可公开获取的来源（如果有）；

(g)本条例第 22 条第 1 款及第 4 款所规定的包括识别分析在内的自动化决策的存在，同时在这些情况下，至少提供关于决策中所运用的逻辑的有用信息以及该处理的重要性和其对数据主体造成的可能后果。

3.数据控制者应当提供本条第 1 款和第 2 款规定的信息：

(a)在获取个人数据后的合理期限内，考虑到个人数据处理的具体情形， 至多不得超过一个月；

(b)如果个人数据是用于联系数据主体的，至迟应于第一次联系数据主体时予以提供；

(c)如果意欲向其他数据接收者披露个人数据，至迟应于个人数据被首次披露时予以提供；

4.当数据控制者意图基于不同于数据收集初始目的的其他目的处理数据时， 数据控制者应当在进行进一步处理之前向数据主体提供有关新目的的信息以及本条第 2 款所规定的所有相关信息。

5.第 1 款到第 4 款的规定不适用于以下情形：

(a)数据主体已获知相关信息；

(b)提供相应信息被证明是不可能或者需要投入过多不必要精力的，尤其是数据处理是出于实现公共利益、科学研究、历史研究或统计的目的，并受本条例第 89 条第 1 款的条件和安全保障措施的约束，或者是本条第 1 款规定的义务可能被认为是不可能的或会严重阻碍数据处理目的实现的。在这些情况下，数据控制者应当采取适当的措施保护数据主体的权利、自由和合法利益，措施包括将信息公之于众；

(c)数据控制者所服从的欧盟或成员国法律已经对数据控制者获取或披露个人数据的行为作了明确规定，且这些法律为保护数据主体的合法利益提供了适当措施；

(d)依据欧盟或成员国法律关于职业保密义务的规定，其中包括法定的保密义务，必须保密的个人数据。

第十五条　数据主体的访问权(Right of access)

1.数据主体有权从数据控制者处获得有关他或她的个人数据是否被处理的确认结果。个人数据被处理的，数据主体有权访问个人数据和以下信息：

(a)处理数据的目的；

(b)相关个人数据的类别；

(c)已经或者将要将个人数据向其披露(disclosed)的数据接收者或其分类，特别是第三国或国际组织的数据接收者；

(d)若有可能，访问个人数据将被存储的预设期限；若不可能，访问决定期限的通常标准；

(e)数据主体享有请求数据控制者更正、清除与数据主体相关的数据的权利，或者限制、拒绝其处理该个人数据的权利；

(f)向监管机构投诉(complaint)的权利；

(g)若个人数据并非收集自数据主体，则可以访问有关数据来源的任何可获得的信息；

(h)本条例第 22 条第 1 款及第 4 款所规定的包括识别分析在内的自动化决策的存在，同时在这些情况下，至少可以访问关于决策中所运用的逻辑的有用信息以及该处理的重要性和其对数据主体造成的可能后果。

2.当向第三国或某一国际组织转移个人数据时，数据主体应当有权被告知本条例第 46 条规定的在转移时应当采取的适当安全保障措施。

3.数据控制者应当提供正在处理的个人数据的副本。对数据主体进一步要求获得副本的请求，

数据控制者可以要求其支付合理的管理费用。数据主体通过电子方式提出申请的，数据控制者也应当以通用的电子方式提供信息。

4.第 3 款规定的索要副本的权利不应对他人的权利和自由产生不利影响。

第三节 更正和清除

第十六条 更正权

数据主体有权要求数据控制者立即更正与其有关的错误的个人数据。考虑到数据处理的目的，数据主体有权要求完善其不完整的个人数据，包括以补充声明的方式完善。

第十七条 清除权(被遗忘权）(Right to erasure (right to be forgotten))

1.在以下情形中，数据主体有权请求数据控制者立即清除与其相关的个人数据，同时数据控制者有义务立即清除相关个人数据：

(a)数据对于收集或处理时的目的已经不再必要；

(b)数据主体撤销对本条例第 6 条第 1 款(a)项或第 9 条第 2 款(a)项规定的个人数据处理的同意，并且没有其他支持个人数据处理的法律依据时；

(c)数据主体依据第 21 条第 1 款的规定行使拒绝权且数据处理没有其他更优法律依据时，或者数据主体依据第 21 条第 2 款的规定行使拒绝权；

(d)个人数据被非法处理；

(e)当数据控制者基于遵守欧盟或成员国法定义务而清除个人数据；

(f)个人数据的收集涉及第 8 条第 1 款规定的提供社会服务信息时。

2.当数据控制者已经公开个人数据的情况并且有义务根据本条第 1 款的规定清除个人数据时。考虑到现有技术和实施成本，数据控制者应当采取包括技术手段在内的合理措施，将数据主体要求清除的有关个人数据的链接、副本和备份等告知正在处理该个人数据的数据控制者。

3.第 1 款和第 2 款的规定不适用于处理确有必要的情况：

(a)行使言论和信息自由权；

(b)当数据控制者基于遵守欧盟或成员国法定义务而处理个人数据，或数据控制者为公共利益而履行义务或者为行使其职务权限进行的数据处理；

(c)为了遵守第 9 条第 2 款(h) (i) 项和第 9 条第 3 款规定的公共健康领域的公共利益进

行的数据处理

(d)根据第 1 款规定为了实现公共利益存档目的、科学研究或历史研究目的或统计目的而进行的数据处理，并且对于本条第 1 款规定的权利的行使会使这些处理的目的变得不可能或被严重损害;

(e)为提起诉讼或应诉所必要的数据处理。

第十八条　限制处理权

1.发生以下情形时，数据主体有权限制数据控制者的处理行为:

(a)当数据主体对个人数据的准确性提出质疑，数据控制者需要一段时间核实数据的准确性;

(b)数据处理违法、数据主体仅要求限制数据使用而反对清除个人数据;

(c)当数据控制者基于处理目的不再需要个人数据，但这些个人数据是数据主体提起诉讼或应诉所必要的;

(d)数据主体可以根据第 21 条第 1 款规定行使拒绝权直到确认了控制者的合法理由优于数据主体。

2.除存储外，在本条第 1 款规定的数据处理受限制的情况下，仅得在经数据主体同意后处理数据，或为提起诉讼或应诉，或为保护其他自然人、法人权利， 或为欧盟或成员国重要公共利益而处理数据。

3.在本条第 1 款规定的个人数据处理受到限制的情况下，数据控制者应当在限制处理落实前通知数据主体。

第十九条　关于更正、清除个人数据或限制处理的通知义务

除非证明此种告知是不可能的或者需要付出不合理的努力，数据控制者应当依据本条例第 16 条、第 17 条第 1 款和第 18 条的规定将任何更改、清除和限制处理的情况告知个人数据公开后的接收者。数据控制者应当在数据主体要求的情况下告知其这些数据接收者。

第二十条　数据的持续控制权(Right to data portability)

1.满足以下情形时，如果数据主体向某数据控制者提供了与其有关的个人数据，那么该数据主体有权从该数据控制者处获取结构化、通用化和可机读的上述数据；同时，数据主体有权将这些数据转移给其他的数据控制者，原数据控制者不得进行阻碍:

(a)当处理是基于第 6 条第 1 款(a)项数据主体同意的情况下或基于第 9 条第 2 款(a)项的规定或基于第 6 条第 1 款(b)项合同约定的情况下;

(b)通过自动化方式进行处理的情况下。

2.基于本条第 1 款规定行使数据持续控制权的数据主体，在技术可操作的情况下有权将相关个人数据从一个控制者处直接转移给另一个控制者。

3.本条第 1 款规定的权利行使不得影响本法第 17 条规定的权利。该权利不适用于为执行公众利益任务所必要或者数据控制者为行使其职务权限进行的数据处理的情况。

4.第 1 款所述的权利，不应对他人权利和自由产生不利影响。

第四节 拒绝权与自动化的个人自决(Automated Individual Decision Making)

第二十一条 拒绝权

1.数据主体有权基于其自身特殊情况随时拒绝依据本法第 6 条第 1 款(e)和(f)项规定而实施的涉及其个人的数据的处理行为，其中包括识别分析行为。除非数据控制者能够证明处理数据的合法依据优先于数据主体的利益、权利与自由或数据处理为提起诉讼或应诉所必要，数据控制者不得继续处理个人数据。

2.若个人数据处理是用于直销(direct marketing)的目的，数据主体有权随时拒绝为此类营销目的而处理其个人数据的行为，包括一定程度上关联到这种直销的分析行为。

3.当数据主体拒绝为直销目的而处理其个人数据时，该个人数据不应再因这种目的而被处理。

4.在第一次告知数据主体的时候，明确提请数据主体注意本条第 1 款和第 2 款所述权利，同时应当将此信息与其他信息分开列明提供给数据主体。

5.无论《电子通信中的隐私保护指令》(Directive 2002/58/EC)如何规定， 在使用信息社会服务的背景下， 数据主体可以通过使用技术规范的自动化方式来行使拒绝权。

6.除了为执行公众利益任务所必要的数据处理，数据主体有权基于其自身特殊情况随时拒绝根据第 89 条第 1 款的规定为科学研究或历史研究目的、统计目的而进行的处理行为。

第二十二条 自动化的个人自决，包括识别分析(Automated individual decision-making, including profiling)

1.数据主体有权不受仅基于自动化处理行为得出的决定的制约，以避免对个人产生法律影响或与之相类似的显著影响，该自动化处理包括识别分析。

2.第 1 款的规定不适用以下决定:

(a)为缔结、履行以数据主体和数据控制者为当事人的合同所必要;

(b)经数据控制者遵守的欧盟或成员国法律授权，且该法律规定了适当的措施以保障数据主

体的权利、自由和合法利益；

(c)基于数据主体明确同意。

3.在本条第 2 款(a)和(c)项规定的情况下，数据控制者应当采取适当的措施以保障数据主体的权利、自由和合法利益，至少应保障数据主体对数据控制者的决定进行人为干预来表达其观点以及对决定提出质疑的权利。

4.本条第 2 款所述决定非以第 9 条第 1 款规定的特殊类型的个人数据为基础，除非适用第 9 条第 2 款(a)或(g)项规定以及采取适当的措施以保障数据主体的权利、自由和合法利益。

第五节 限制

第二十三条 限制

1.数据控制者和处理者遵守的欧盟或成员国法律可以通过立法手段限制本法第 12 至 22 条和第 34 条规定的权利义务范围，对于第 5 条中符合第 12 至 22 条规定的权利义务的条款也同样适用，当此类限制具有尊重基本权利和自由的本质且在民主社会中对保护以下事项是必要且适当的：

(a)国家安全；

(b)防卫；

(c)公共安全；

(d)预防、调查、侦查和起诉犯罪或执行刑罚，包括应对和预防威胁公共安全的安全保障措施；

(e)维护欧盟或某一成员国其他重要公共利益，特别是欧盟或某一成员国的重要经济或金融利益，包括货币、预算和税收事务、公共健康和社会安全事务；

(f)保护司法独立和司法程序；

(g)预防、调查、侦查和起诉违反职业道德规范的行为；

(h)与本条(a)至(e)和(g)项规定的行使公权力相关的监控、检查或监管行为，即使这种关联是偶然的；

(i)保护数据主体或者他人的权利和自由；

(j)行使民法上的请求权；

2.本条第 1 款中规定的立法手段应当至少包括一些相关的具体条款，尤其是相关的时候，

包括:

(a)处理目的或处理类别;

(b)个人数据的种类;

(c)出台的限制的范围;

(d)预防滥用和非法访问或转移个人数据的安全保障措施;

(e)控制者的说明或控制者类别;

(f)存储期限以及考虑到处理的性质、范围、目的或处理的类别而适用的安全保障措施;

(g)对数据主体权利和自由带来的风险;

(h)除非可能会损害限制的目的，应当告知数据主体权利受限制的情况。

第四章　数据控制者和数据处理者

第一节 一般义务

第二十四条　数据控制者的责任

1.考虑到处理行为的性质、范围、环境、目的以及可能对自然人的权利和自由带来的风险和损害,数据控制者应当采取适当的技术和组织措施以确保并证明处理行为是按照本法的规定进行的。这些措施应当在必要的情况下进行评估和更新。

2.当要和处理行为相称时，第 1 款所规定的措施应当包括数据控制者实施的适当的数据保护政策。

3.遵守本法第 40 条规定的行为准则或第 42 条规定的认证机制可作为证明其履行了数据控制者义务的要件。

第二十五条 数据系统保护和默认保护(data protection by design and by default)

1.考虑到国家的发展水平、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，例如设计来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到处理之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。

2.数据控制者应当实施相应的技术和组织措施以确保在默认(by default)情形下，被处理的个人数据对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。

3.第 42 条规定的认证机制可作为证明其行为符合本条第 1 和第 2 款的规定的要件。

第二十六条　共同的数据控制者

1.共同数据控制者是指共同决定数据处理目标、条件和手段的两个或两个以上数据控制者。除非欧盟和成员国已经规定了数据控制者作为主体分别负担各自的责任外，他们应当共同以一种透明的方式安排其各自的责任以履行本法所规定的各项义务，尤其涉及数据主体行使权利和本法第 13 条和第 14 条规定的各自通知义务。数据控制者的安排应当包括为数据主体指定一个联络点。

2.本条第 1 款所规定的内部安排应当完全反映各自的职责以及面对数据主体时共同数据控制者的关系。安排的实质内容应被数据主体获知。

3.不论第 1 款所述的内部安排如何规定，数据主体都可以根据本条例相关规定向每一位数据控制者行使权利。

第二十七条　设立于欧盟外的数据控制者或处理者的代表人

1.在本条例第 3 条第 2 款规定的情形下，数据控制者或处理者应当以书面形式在欧盟境内指派一位代表人。

2.此项义务不适用于以下情况：

(a)偶尔的处理行为，不包括第 9 条第 1 款规定的对特殊个人数据的大规

模处理或第 10 条规定的有关刑事违法和定罪的数据处理。此外考虑到处理行为的性质、环境、范围和目的，该处理行为对自然人的权利和自由产生风险的可能性较小；或

(b)公共机关或团体。

3.代表人应当设立在这样的成员国内：个人数据被处理以向其提供商品或服务，或者其行为被监控的数据主体所在的国家。

4.为了确保遵守本法之规定，特殊情况下与数据处理有关的争议需要由监管部门和数据主体授权代表人，一般情况下代表人由数据控制者或处理者授权。

5.数据控制者或处理者指派代表人的行为不影响对数据控制者和处理者提起的法律诉讼。

第二十八条　数据处理者

1.在代表数据控制者实施数据处理操作的情形中，数据控制者所使用的数据处理者必须提供充分保障以实施适当的技术、组织措施使数据处理满足本条例的要求并确保数据主体的权利得到保护。

2.在没有事先获得数据控制者的特别或一般书面授权时，数据处理者不得招募(engage)另一个数据处理者。在获得一般书面授权的情况下，数据处理者应当告知数据控制者任何有关增加或替换其他数据处理者的预期变动，以给数据控制者拒绝上述变动的机会。

3.数据处理者的处理行为应当受到合同或者欧盟或各成员国法律规定的法律行为(legal act)的约束，该合同或其他法律行为对数据处理者和控制者具有法律约束力，并且确立了处理行为的内容和期限、性质和目的，个人数据的类型和数据主体的种类以及数据控制者的权利与义务。上述合同或其他法律行为应当规定数据处理者如下行为：

(a)只能根据数据控制者记载的指示进行个人数据的处理，包括向第三国或国际组织转移个人数据，除非是可适用于数据处理者的欧盟或各成员国法律要求这么做；在上述情况下，数据处理者应当在处理前将法律要求告知数据控制者， 除非法律基于重要的公共利益禁止披露前述信息；

(b)确保被授权处理个人数据的人已经承诺保密或负有适当的法定保密义务；

(c)采取第 32 条规定的所有措施；

(d)遵守本条第 2 款和第 4 款规定的招募另一个数据处理者的条件要求；

(e)考虑到处理的性质，在可能的情况下，以适当的技术和组织措施协助数据控制者，使数据控制者履行法定义务，确保数据主体得以行使本条例第三章规定的权利。

(f)协助数据控制者，确保其履行本条例第 32 至 36 条规定的义务，考虑到处理的性质和数据处理者可获取的信息；

(g)根据数据控制者的选择，在完成有关处理的服务后删除或收回所有发给控制者的个人信息，并删除现存副本，除非欧盟或成员国法律要求保存这些个人数据；

(h)使得数据控制者可以获取一切必要信息以证明数据处理者履行本条中规定的义务，允许并促成(allow for and contribute to)审计工作的开展， 包括由数据控制者或其指定的另一审计员进行的调查工作。

根据第 1 款(h)项的规定，如果数据处理者认为数据控制者的指示违反了本条例或其他欧盟或成员国数据保护法律的规定，其应当立即通知数据控制者。

4.当数据处理者招募另一个数据处理者来代表数据控制者实施特定的处理活动，其他数据处理者同样也要通过合同或是欧盟或各成员国法律规定的其他法律行为的方式遵守本条第 3 款规定的数据控制者与处理者之间的合同或其他法律行为要求的数据保护义务，尤其要提供

充分保障以实施适当的技术和组织措施以满足本条例的要求。当另一个数据处理者未能遵守他的数据保护义务时，原先的数据处理者应当就该数据处理者的义务履行行为向数据控制者承担全部责任。

5.可以将数据处理者对第 40 条规定的已被认可的行为准则或第 42 条规定的已被认可的认证机制的遵守情况作为证明本条第 1 款和第 4 款规定的要求的因素。

6.在不影响数据控制者和处理者之间的个别合同(individual contract)的情形下，本条第 3 款或第 4 款规定的合同或其他法律行为可以全部或部分地以本条第 7 款和第 8 款规定的标准合同条款为基础，包括当这些条款是作为按照第

42 条和第 43 条的规定授予控制者或处理者认证资格的一部分时。

7.委员会应当为本条第 3、4 款中涉及到的情形制定标准合同条款，并且遵守第 93 条第 2 款规定的审查程序(examination procedure)。

8.在涉及本条第 3、4 款的情形时，监管机构可以适用标准合同条款，并遵守第 63 条规定的一致性机制。

9.第 3、4 款规定的合同或其他法律行为应当采用书面的形式，包括电子形式。

10.在不影响第 82、83 和 84 条的情形下，如果数据处理者违反本条例的规定自行决定处理的目的和方式，则其应当被视为是此次处理行为的数据控制者。

第二十九条　数据控制者或处理者授权的处理

除非欧盟或成员国法律有所要求，数据处理者和依据对个人数据享有访问权限(have access to)的数据控制者或数据处理者的授权行事的任何人，非经数据控制者的指示不得处理数据。

第三十条　处理活动的记录(Records of processing activities)

1.每一个数据控制者及其代表人（如果有），应当保存一份由其负责的数据处理活动的记录。该记录应当包含所有以下信息：

(a)数据控制者以及共同数据控制者、控制者的代表人和数据保护专员（ 如果有）的姓名和联系方式；

(b)处理的目的；

(c)对数据主体类型和个人数据类型的描述；

(d)已经或将要接收个人信息披露的数据接收者的分类，包括在第三国或国际组织的接收者；

(e)如果可能，向第三国或国际组织转移个人数据的情形中的第三国或国际组织的身份信息，

以及第 49 条第 1 款第 2 段规定的转移情形中的适当安全保护措施的证明文件;

(f)如果可能，清除不同类型数据的预计期限;

(g)如果可能，关于第 32 条第 1 款规定的技术性与组织性安全措施的一般描述;

2.每个数据处理者以及处理者的代表人（如果有），应当保存一份关于所有其代表数据控制者实施的处理活动的记录，记录包含如下内容:

(a)一个或多个数据处理者、每个处理者代表的数据控制者以及数据控制者或处理者的代表人和数据保护专员（如果有）的姓名和联系方式;

(b)代表每个数据控制者实施的处理行为的种类;

(c)如果可能，向第三国或国际组织转移个人数据的情形中的第三国或国际组织的身份信息，以及第 49 条第 1 款第 2 段规定的转移情形中的适当安全保护措施的证明文件;

(d)如果可能，关于第 32 条第 1 款规定的技术性与组织性安全措施的一般描述。

3.第 1、2 款规定的记录应当采用书面形式，包括电子形式。

4.数据控制者或处理者以及，数据控制者或处理者的代表人（如果有），经监管机构的要求应当向其提供该记录。

5.第 1、2 款规定的义务不得适用于雇员人数少于 250 人的企业或组织，除 非其实施的处理可能对数据主体的权利与自由产生风险，或是该处理不是临时的， 或是该处理内容包括了第 9 条第 1 款规定的特殊种类的数据或第 10 条规定的与刑事定罪和犯罪有关的数据。

第三十一条　与监管机构合作

数据控制者和处理者以及他们的代表人（如果有），经请求，应当与监管机构合作履行其职责。

第二节 个人数据的安全

第三十二条　处理安全

1.考虑到各国国内发展水平、实施成本和数据处理的性质、范围、内容和目的以及对自然人权利与自由带来风险的可能性(varying likelihood)与严重性， 数据控制者和处理者应当实施适当的技术和组织措施以确保安全水平与风险程度相一致，尤其包括如下内容:

(a)个人数据的假名化机制和加密措施;

(b)确保处理系统和服务能够持续保持自身保密性，完整性，有效性和自我修复

(confidentiality,integrity,availability and resilience)的能力；

(c)在物理性或技术性事故中及时恢复个人数据的有效性和对个人信息访问的能力；

(d)实施一项定期测试、评估、评价技术性和组织性措施有效性的程序以确保处理的安全性。

2.为评估安全性的适当水平，尤其应当考虑处理行为所表现出来的风险，尤其是意外的或非法的损毁、丢失、修改、未经授权的披露或访问转移中的、存储中的或其他处理过程中的个人数据。

3.可以将数据控制者或处理者对第 40 条规定的已被认可的行为准则或第 42 条规定的已被认可的认证机制的遵守情况作为证明遵守本条第 1 款规定的要求的因素。

4.除非欧盟或各成员国法律有所要求，数据控制者和处理者应当采取措施以确保任何依据对个人数据享有访问权限的数据控制者或处理者的授权行事的自然人非经数据控制者的指示不得处理这些数据。

第三十三条　向监管机构报告个人数据泄露的义务

1.在发生个人数据泄露的情形时，数据控制者应当自发现之时起 72 小时内，按照第 55 条的规定将个人数据泄露的情况报告监管机构，除非该个人数据的泄

露不太可能会对自然人的权利和自由造成风险。未能在 72 小时内报告的，则需要说明未及时报告的理由。

2.数据处理者应当在发现个人数据泄露后立即通知数据控制者。

3.本条第 1 款中所称的报告至少应包括以下内容：

(a)阐述个人数据泄露的性质，包括所涉数据主体的种类和大致数量，以及所涉数据记录的种类和大致数量；

(b)告知数据保护专员的姓名和具体联系方式，或其他能够获取更多信息的联系方式；

(c)阐述个人数据泄露可能导致的结果；

(d)阐述数据控制者提议或采取的处理个人数据泄露的措施，还应包括减少个人数据泄露可能导致的不利影响的措施（如果有）。

4.到了这一阶段，如果数据控制者不能同时提供上述所有信息，也需要毫无延迟地分阶段提供这些信息。

5.数据控制者应当记录下所有的个人数据泄露事件，记录应包括个人数据泄露有关的事实、影响及采取的补救措施。该记录必须使监管机构能够核实该记录是符合本条规定的。

第三十四条　向数据主体告知个人数据泄露的义务

1.当个人数据泄露可能对自然人的权利和自由产生较高风险时，数据控制者应当立即将个人数据泄露的事实告知数据主体。

2.本条第 1 款规定的告知义务应当用明确和清楚的语言说明个人数据泄露的性质并且至少包含本条例第 33 条第 3 款(b) (c) 和(d) 项的信息和建议。

3.在符合以下条件时，无需履行本条第 1 款规定的告知义务：

(a)数据控制者已经实施了相应的技术性和组织性保护措施，并且这些措施已经被应用在被泄露的个人数据上，尤其是这种保护措施使得个人数据不被任何未经授权的访问者所接触，例如加密技术；

(b)数据控制者已经采取了后续的措施确保第 1 款中规定的对数据主体权利和自由产生的高风险不再可能成为现实；

(c)在涉及不合理的工作比例时，在这种情形下，取而代之的是应当通过大众传媒或者类似的手段来使数据主体获得同样有效的告知。

4.如果数据控制者没有向数据主体告知数据泄露，监管机构在考量个人数据泄露导致高风险的可能性后，可以要求数据控制者履行告知义务，或者决定是否符合第 3 款规定的某一条件。

第三节 数据保护影响评估和事先咨询

第三十五条　数据保护影响评估

1.当一种处理行为特别是用到了新技术时，考虑到处理行为的性质、范围、内容和目的可能会对自然人的权利和自由产生高风险时，数据控制者应当在处理前完成一份设想的数据处理对个人数据保护影响的评估。一份评估可以提出存在相似高风险的一套类似的处理行为。

2.数据控制者在实施数据保护影响评估时，在指定的情形下应当征询数据保护专员的建议。

3.在以下情形中尤其需要第 1 款规定的数据保护影响评估：

(a)基于数据的自动化处理包括识别分析(profiling)，或者基于对该自然人产生法律效力或者类似的显著影响的决定，对自然人个人方面的系统和广泛的评估；

(b)处理大规模的第 9 条第 1 款规定的特殊类型的数据，或大规模的第 10 条规定的有关犯罪记录和违法行为的个人数据；或者

(c)对公共区域大规模的系统化监控。

4.监管机构应当确定并公开一份清单，列举应当按照第 1 款规定进行数据保护影响评估的处理行为。监管机构应当将清单告知第 68 条规定的欧洲数据保护委员会。

5.监管机构同样要确定并公开一份清单，列举不需要进行数据保护影响评估的处理行为。监管机构也应将该清单告知欧洲数据保护委员会。

6.在采用第 4 款和第 5 款规定的清单前，若清单涉及向数据主体提供商品或服务的处理行为，或在多个成员国监控他们的行为的处理行为，或可能对个人数据在欧盟境内的自由流通产生实质影响的处理行为，监管机构应当适用第 63 条规定的一致性机制。

7.评估内容至少应当包括如下方面：

(a)对于设想中的处理行为和处理行为的目的系统化的说明，适当的情况下还包括控制者追求的合法利益；

(b)基于处理目的，对处理行为的必要性和相称性的评估；

(c)对于第 1 款中规定的对数据主体权利和自由产生的风险的评估；

(d)处理这些风险的预想方案，包括安全和保障措施，以及确保个人数据的保护和证明符合本条例规定的机制。以上方案应当考虑数据主体和其他相关人员的权利和合法利益。

8.在对数据控制者或处理者进行的处理行为进行影响评估时，尤其是为了达到数据保护影响评估的目的，应当考虑该数据控制者或处理者对第 40 条规定的行为准则的遵守情况。

9.在适当的情况下，数据控制者应当就打算的处理行为征询数据主体或其代表人的意见，公正地对待商业保护或公共利益或处理行为的安全性。

10.依据第 6 条第 1 款(c)项和(e)项进行的处理行为在数据控制者所遵守的欧盟或成员国法律中具有法律依据，这些法律规定了某一具体处理行为或者一系列处理行为，并且在适用上述法律依据时已经实施了一项作为一般影响评估一部分的数据保护影响评估，该种情况下不适用本条第 1 到 7 款的规定，除非成员国认为在处理活动前实施数据保护影响评估是有必要的。

11.必要的时候，至少是当处理行为出现风险变化的时候，数据控制者应当进行复审以评估数据处理行为是否符合数据保护影响评估。

第三十六条　事先咨询

1.当根据第 35 条制定的数据保护影响评估表明在控制者缺乏减轻风险的措施会导致高风险时，数据控制者应当在处理前向监管机构咨询。

2.当监管机构认为即将实施的第 1 款中规定的处理行为会违反本条例，尤其是数据控制者

不能确定和减少风险时，监管机构应当在收到咨询请求后八周的期限内，向数据控制者提供书面建议，并且也适用于数据处理者和按照第 58 条规定行使职权的任何人。考虑到即将实施的处理行为的复杂性，这一期限可以延长六周。监管机构应当在收到咨询请求的一个月内将任何延期和延期的原因告知数据控制者和处理者（如果有）。这些期限可以暂停，直到监管机构获得了基于咨询目的所要求的信息。

3.当按照第 1 款向监管机构咨询的时候，数据控制者应当向监管机构提供以下信息：

(a)处理过程中涉及的控制者、共同控制者和处理者（如果有）各自的责任，尤其是当处理发生在企业集团内部的时候；

(b)打算实施的处理行为的目的和方法；

(c)按照本条例所采取的保护数据主体权利和自由的保障措施；

(d)数据保护专员的联系方式（如果有）；

(e)第 35 条要求的数据保护影响评估；以及

(f)监管机构要求的任何其他信息。

4.成员国在向其国内议会提交有关数据处理行为的立法议案或依据该立法制定行政规制措施时，应当向监管机构咨询。

5.尽管存在第 1 款规定，但当数据控制者为执行与公共利益有关的任务进行数据处理时，包括与社会保障和公共安全有关的处理，成员国法律可以要求数据控制者向监管机构咨询并且征得其事先授权。

第四节 数据保护专员

第三十七条 数据保护专员的指定

1.在以下情形中，数据控制者和数据处理者应当指定一名数据保护专员：

(a)当数据处理是由行政机关或公共团体实施时，除了法院在其司法职能内的行为；

(b)数据控制者和数据处理者的核心业务由数据处理组成，该处理因其自身的性质、范围和/或目的等需要对数据主体进行定期的、系统化的大规模监控； 或者

(c)数据控制者和处理者的核心业务由处理第 9 条规定的大规模特殊类型的数据和第 10 条规定的与犯罪记录和违法行为有关的数据组成。

2.若该专员能够轻易接触到每个部门，一个企业集团可以只任命一个数据保护专员。

3.当数据控制者或处理者是行政机关或公共团体时，考虑到他们的组织机构和规模，可以为多个机关和团体指定一名数据保护专员。

4.除了本条第 1 款所列情形外，数据控制者和数据处理者以及其他代表各类数据控制者和处理者的团体和机构(associations and other bodies)也可以按照欧盟或者成员国法律的要求，指定一名数据保护专员。该专员可以代表上述团体和机构履行职责。

5.数据保护专员的指定应当建立在专业素养，尤其是对数据保护法律的专业知识和实践，以及履行第 39 条规定的任务的能力基础上。

6.数据保护专员可以是数据控制者或处理者的员工，也可以按照服务合同来完成任务。

7.数据控制者或处理者应当公开数据保护专员的联系方式，并且告知监管机构。

第三十八条　数据保护专员的地位

1.数据控制者或数据处理者应当确保数据保护专员恰当、及时地参与所有有关个人数据保护的事务

2.数据控制者和处理者应当通过提供执行这些任务所必要的资源，个人数据和处理行为的访问途径，以及维持他或她的专业知识等途径，支持数据保护专员执行第 39 条规定的任务。

3.数据控制者和处理者应当确保数据保护专员不会收到任何有关执行其工作任务的指示。他或她不能因执行自身的任务而被解雇或处罚。数据保护专员应当直接向数据控制者或处理者的最高管理层报告。

4.数据主体可以就有关处理其个人数据和行使本条例规定的权利的所有问题联系数据保护专员。

5.依据欧盟或成员国的法律，数据保护专员对其工作任务的执行有保密义务。

6.数据保护专员可以履行其他任务和职务，数据控制者或处理者应当确保任何这样的任务和职务都不能导致利益冲突。

第三十九条　数据保护专员的任务

1.数据保护专员至少应当有以下任务:

(a)向数据控制者或处理者和有义务按照本条例或者其他欧盟或成员国数据保护条款实施处理行为的雇员发出通知或建议;

(b)监督本条例的遵守情况，和其他欧盟或成员国数据保护条款以及控制者或处理者有关个人数据保护的政策的遵守情况，包括责任的分配、意识的提升、参与处理行为的员工的培训以及相关的审计;

(c)应要求提供有关数据保护影响评估的建议并根据第 35 条的规定监督评估工作的实施;

(d)与监管机构保持协作;

(e)在有关数据处理的问题中充当监管机构的联络点，包括第 36 条规定的事先咨询和有关任何其他事务的咨询（如果有）。

2.数据保护专员应当在履行他或她的职责时,从处理行为的性质、范围、环境以及处理目的的角度合理关注数据处理行为中伴随的风险。

第五节 行为准则与认证

第四十条 行为准则

1.成员国、监管机构、欧洲数据保护委员会和欧盟委员会应当鼓励拟定行为准则，以促进本条例的合理实施。制定行为准则时，应当考虑到各类数据处理领域的具体特点以及微型、小型和中型企业的具体需求。

2.代表各类数据控制者或处理者的机构和协会可以起草行为准则，也可以修改或扩展这些准则来明确本条例的适用，如:

(a)公平、透明的数据处理;

(b)在特定情况下数据控制者追求的合法利益;

(c)个人数据的收集;

(d)个人数据的假名化;

(e)提供给公众和数据主体的信息;

(f)数据主体权利的行使;

(g)提供给儿童的信息、对儿童的保护，以及对儿童具有家长责任的人的同意的获取方式;

(h)第 24 条和第 25 条规定的措施和程序以及第 32 条规定的确保处理行为安全的措施;

(i)向监管机构报告个人数据的泄露以及将该泄露告知数据主体;

(j)将个人数据向第三国或国际组织的转移;

(k)用以解决数据控制者和数据主体之间关于处理行为争议的庭外程序和其他争议解决程序,公正地保护第 77 条和第 79 条中数据主体的权利。

3.为了依据第 46 条第 2 款(e)项规定，对向第三国或国际组织转移个人数据提供适当的安全保障措施，除了受本条例约束的数据控制者和处理者需遵守之外，根据本条第 5 款批准的行为准则以及本条第 9 款规定的一般有效性，也应被第 3 条规定的不属于本条例调整范围内的数据控制者或处理者所遵守。这类数据控制者或处理者应当通过合同条款或者其他具有法律约束力的文件作出具有约束力和执行力的承诺，来适用这些适当的安全保障措施，包括与数据主体的权利相关的安全保障措施。

4.本条第 2 款规定的行为准则应当包含确保第 41 条第 1 款规定的机构能够强制监控数据控制者或处理者遵守条款的机制，并且不得影响依据第 55 条或第 56 条的规定有权限的监管机构的任务和职权。

5.本条第 2 款中规定的协会或其他机构准备起草行为准则或修改、扩展现有的准则时，应当将准则的草案、修正案或扩展方案提交给依据第 55 条规定的有权的监管机构。监管机构应当就该准则草案、修正案或扩展方案是否符合本条例 给出意见，并且在证实其已经提供了充分的适当安全保障措施后批准该准则草案、修正案或扩展方案。

6.当准则草案、修正案或扩展方案按照第 5 款规定被批准，并且行为准则的内容不涉及在多个成员国进行的数据处理时，监管机构应当登记并公布该准则。

7.当起草的准则涉及在多个成员国进行的数据处理时，根据第 55 条规定的

有权监管机构应当在批准该准则草案、修正案或扩展方案前按照第 63 条的程序将其提交给欧洲数据保护委员会，委员会应当就该准则草案、修正案或扩展方案是否符合本条例或在第 3 款规定的情况下是否提供了适当的安全保障措施给出意见。

8.如果第 7 款规定的意见确认了该准则草案、修正案或扩展方案符合本条例的规定，或者在第 3 款规定的情况下，提供了适当的安全保障措施时，欧洲数据保护委员会应当将其意见提交给欧盟委员会。

9.欧盟委员会可以通过实施性法令来决定根据第 8 款规定提交给它的已经被批准了的准则草案、修正案或扩展方案在欧盟范围内具有普遍的效力。实施性法令的制定应当符合本条例第 93 条第 2 款所规定的审查程序。

10.欧盟委员会应当确保对第 9 款规定的已经被批准且确定具有普遍约束力的准则进行适当的宣传。

11.欧洲数据保护委员会应当核对所有登记的被批准的行为准则、修正案或扩展方案，并且应当确保它们能被公众通过任何适当的方式所知悉。

第四十一条　对被批准的行为准则的监控

1.在不影响第 57 条和第 58 条规定的有权监管机构的任务和职权的前提下，对第 40 条规定的行为准则的遵守的监控可以由有权监管机构认证的、对准则的主要问题拥有适当专业水

准的机构来实施。

2.第 1 款中规定的机构在具备以下条件时可以被认证，以监控行为准则的遵守：

(a)证明了它的独立性和有关准则主要问题的专业水准满足了有权监管机构的要求；

(b)已建立程序，使其可以评估适用行为准则的数据控制者和处理者的资格，可以监控他们遵守行为准则条款的情况和定期审查他们的操作；

(c)已建立程序，以处理针对违反准则的行为或对数据控制者或处理者已经或正在实施准则的方式的投诉，并且向数据主体和公众公开这些程序；并且

(d)证明了他们的任务和职责不会导致利益冲突并且满足有权监管机构的要求。

3.有权监管机构应当将起草的认证本条第 1 款中规定的机构的标准按照第

63 条规定的一致性机制提交给欧洲数据保护委员会。

4.在不影响有权监管机构的任务和职权以及第八章的条款时，第 1 款中规定的机构应当遵守适当安全保障措施，在数据控制者或处理者违反准则时采取适当措施，包括暂停或排除准则涉及的控制者或处理者的权限。同时也应将上述行为以及采取上述行为的原因告知有权的监管机构。

5.不满足或不再满足认证条件或该机构的行为违反本条例规定时，有权监管机构应当撤回第 1 款中规定的对于机构的认证。

6.本条不适用于公共机构和组织实施的处理行为。

第四十二条　认证

1.为了证明数据控制者或处理者的数据处理行为符合本条例的规定，成员国、监管机构、欧洲数据保护委员会以及欧盟委员会应当倡导，特别是在欧洲范围内，　建立数据保护认证机制以及数据保护印章和标志，同时应当考虑到微型、小型和 中型企业的具体需求。

2.除了受本条例约束的数据控制者和处理者需遵守之外，根据本条第 5 款批准的数据保护认证机制、印章或标志的设立也是为了证明第 46 条第 2 款(f)项规定的向第三国或国际组织转移个人数据时，根据第 3 条的规定不属于本条例调整对象的数据控制者或处理者也提供了适当安全保障措施。这类数据控制者或处理者应当通过合同条款或者其他具有法律约束力的文件做出具有约束力和执行力的承诺，来适用这些适当的安全保障措施，包括与数据主体的权利相关的安全保障措施。

3.认证应当是自愿的，并且可通过透明的程序获得。

4.根据本条所做的认证不能减少数据控制者或处理者遵守本条例的责任，并且不得影响本条

例第 55 条或第 56 条规定的有权监管机构的任务和职权。

5.本条所规定的认证应当由第 43 条规定的认证机构或有权监管机构基于有权监管机构根据第 58 条第 3 款或欧洲数据保护委员会根据第 63 条批准的条件签发。当条件被欧洲数据保护委员会批准时，可能会产生一个一般认证，即欧洲数据保护印章。

6.控制者或处理者在将他们的处理行为提交给认证机制时，应当向第 43 条规定的认证机构或者有权监管机构（如果有）提供实施认证程序所需的所有信息和访问处理行为的权限。

7.签发给控制者或处理者的认证的有效期限最长为三年，并且在相同的条件下，如果相关要求继续满足，可以续期。认证应当由第 43 条规定的认证机构或者有权监管机构在认证的条件不满足或不再继续满足时撤回。

8.欧洲数据保护委员会应当核对所有认证机制和登记的数据保护印章以及标志，并且确保它们能被公众以任何适当的方式知悉。

第四十三条　认证机构

1.在不影响第 57 条和第 58 条规定的有权监管机构的任务和职权的情况下， 具备有关个人数据保护的专业水准的认证机构在为了使其在必要时能够行使第 58 条第 2 款(h)项规定的职权而通知监管机构后，应当签发和更新认证。成员国应当确保这些认证机构被以下一个或多个机构认可：

(a)本条例第 55 条或者第 56 条规定的有权监管机构；

(b)欧盟议会和理事会颁布的《确立关于产品市场营销的认证与市场监督管理的要求的条例》[Regulation(EC)No 765/2008]指定的，并且符合《合格评定——机构证实产品、操作工序和服务合格的要求》(EN-ISO/IEC 17065/2012) 的规定和本条例第 55 条或第 56 条规定的有权监管机构附加的额外要求的国家认证机构。

2.第 1 款中规定的认证机构只有在以下情形中才能依照第 1 款被认可：

(a)已证明其独立性和有关认证的主要问题的专业知识满足有权监管机构的要求；

(b)已承诺遵守本条例第 42 条第 5 款规定的准则和由第 55 条或第 56 条规定的有权监管机构或由第 63 条规定的欧洲数据保护委员会批准的准则；

(c)已建立签发、定期检查和撤回数据保护认证以及印章和标志的程序；

(d)已建立处理投诉的程序、组织，以处理对认证的违反或数据控制者或处理者实施的正在生效或已经存在的认证方式的投诉，并且使这些程序和组织对数据主体和公众都是公开透明的；

(e)证明他们的任务和职责没有导致利益的冲突并且满足有权监管机构的要求。

3.第 1 款和第 2 款中规定的对认证机构的认可应当建立在由第 55 条或第 56 条规定的有权监管机构或由第 63 条规定的欧洲数据保护委员会批准的准则的基

础上。应当将本条第 1 款(b)项情形中的那些要求作为《确立关于产品市场营销认证与市场监督的要求的条例》[(EC)No 765/2008]规定的要求和描述认证机构的认证方式和程序的技术规则的补充。

4.在不影响数据控制者或处理者遵守本条例的其他责任的情况下，第 1 款中规定的认证机构应当对产生或撤回认证所进行的适当评估负责。签发的认证的最长期限为五年，并且在相同的情况下，只要认证机构满足了本条设立的要求便可以续期认证。

5.第 1 款中规定的认证机构应当向有权监管机构提供同意或撤回认证请求的原因。

6.本条第 3 款中规定的要求和第 42 条第 5 款规定的条件应当由监管机构以一种易接触的形式向公众公开。监管机构还应当将这些要求和条件告知欧洲数据保护委员会，委员会应当核对所有的认证机制和登记的数据保护印章以及确保这些信息都能被公众以任何适当的方式所获得。

7.在不违反第八章的规定的前提下，有权监管机构或者国家认证机构应当在认可的条件不满足或不再满足或认证机构采取的行为违反了本条例的规定时，撤销根据本条第 1 款对该认证机构所做的认可。

8.依据本条例第 92 条的规定，授权欧盟委员会制定第 42 条第 1 款规定的数据保护认证机制的具体要求。

9.欧盟委员会可以通过实施性法令来确定认证机制和数据保护印章、标志的技术标准，并采取完善和认可这些认证机制、印章和标志的机制。这些实施性法令的制定应当符合本条例第 93 条第 2 款所规定的审查程序。

第五章 向第三国或国际组织转移个人数据

第四十四条 转移的总体原则

任何正在转移个人数据的行为或是转移到第三国或国际组织之后意图再转移的行为，只有在数据控制者和处理者满足了本章规定的条件且遵守本条例的其他内容时才能得以实施。前述个人数据转移也包括从第三国或国际组织转移到另一个第三国或国际组织。本章所有条款都应被用来确保本条例保障的对自然人的保护水平不被破坏。

第四十五条 在充分条件基础上的转移

1. 当欧盟委员会决定第三国、第三国的某一地区、某个或多个特定的部门或某国际组织已经确定达到充分的保护标准时，数据便可以向第三国或国际组织转移。这样的数据转移不需

要经过任何特别授权。

2. 在评估保护水平的充分性时，欧盟委员会应当特别考虑以下要素：

（a）法律规则，对于人权和基本自由的尊重，包括涉及公共安全、防卫、国家安全以及刑事法律和公共机构对于个人数据的访问的相关综合性和专门性立法以及这些立法的实施，数据保护规则，职业准则和安全措施，包括第三国或国际组织制定的调整对正在向第三国或国际组织转移个人数据的规则，还包括判例法，有效且可执行的数据主体权利以及有效的行政管理和对个人数据被转移的数据主体的司法救济；

（b）第三国或者国际组织存在一个或多个独立有效运行的监管机构来负责确保数据保护规则的遵守，包括充分的执法权力，以协助和指导数据主体行使他们的权利，也包括与成员国中的监管机构合作；以及

（c）第三国或相关国际组织已经缔结的国际协定，或者其他源于具有法律约束力的公约或文件所规定的义务，或者源于它们参加的尤其是有关个人数据保护的多边或区域体系。

3. 欧盟委员会在评估了保护水平的充分性后可以通过实施条款来决定某第三国或者第三国的某一地区、某个或多个特定部门，或者某国际组织已经满足了本条第 2 款规定的充分保护标准。该实施条款应当设立至少每四年定期检查的机制，并且要考虑到第三国或国际组织所有相关方面的发展进步。该实施条款应当明确它的适用的地域和部门，并且在适当的情况下，确定本条第 2 款(b)项规定的监管机构。该实施条款的采用应当符合本条例第 93 条第 2 款所规定的审查程序。

4. 欧盟委员会应当持续监控第三国和国际组织中可能影响到根据本条第 3 款和《数据保护指令》第 25 条第 6 款所做的决定的运行情况。

5. 依照本条第 3 款的审查制度，当有效信息显示第三国、第三国的某一地区或者一个或多个特定部门、国际组织不再处于本款第 2 条要求的充分保护水平时， 如果必要，委员会应当通过实施法令废除、修订或暂停依据本条第 3 款规定的决定，且这些措施没有溯及力。这些实施法令的采用应当符合本条例第 93 条第 2 款所规定的审查程序。

在证明必要紧急情况下，委员会应当根据第 93 条第 3 款规定的程序立即采取适当的实施法令。

6. 欧盟委员会应当和第三国或国际组织进行磋商以补救依据本条第 5 款作出的决定所导致的后果。

7. 根据本条第 5 款所做的决定，不影响根据第 46 至 49 条进行的将个人数据向第三国、第三国某一地区或该第三国中被指定的一个或多个部门或者国际组织的转移。

8. 欧盟委员会应当将那些达到充分保护水平和未达到充分保护水平的第三国、地区、第三国的特定部门或国际组织的名单列表发布在欧盟的官方公报和它的网站上。

9. 依据《数据保护指令》第 25 条第 6 款所作的决定在被欧盟委员会依据本条第 3 款和第 5 款所作决定修改、替代或废除前仍旧有效。

第四十六条 遵守适当保障措施的转移

1. 在缺乏根据第 45 条第 3 款所做的决定时，数据控制者或处理者只有在提供了适当的保障措施并且满足数据主体能行使权利、能获得有效的法律救济的条件时才能将个人数据向第三国或国际组织转移。

2. 第 1 款中规定的适当保障措施无需监管机构的任何具体授权，可以由以下方式来提供：

（a） 公共当局或机构间的具有法律约束力和执行力的文件；

（b） 符合本条例第 47 条规定的公司约束规则；

（c） 欧盟委员会采用的符合第 93 条第 2 款所规定的审查程序的标准数据保护条款；

（d） 监管机构采用的标准数据保护条款和欧盟委员会依据第 93 条第 2 款所规定的审查程序；

（e） 根据第 40 条批准的行为准则以及第三国数据控制者或处理者具有约束力和执行力的适用适当保障措施的承诺，包括对于数据主体权利的承诺；

（f） 根据第 42 条批准的认证机制以及第三国数据控制者或处理者具有约束力和执行力的适用适当保障措施的承诺，包括对于数据主体权利的承诺。

3. 遵从有权监管机构的授权，第 1 款中规定的适当保障措施也可以由以下方式提供：

（a） 数据控制者、处理者与控制者、处理者或第三国、国际组织中的个人数据接收者之间的合同条款；

（b） 包括数据主体可执行的有效的权利在内的内容被附录在公共当局或机构的行政安排中。

4. 在本条第 3 款规定的情况中，监管机构应当适用第 63 条规定的一致性机制。

成员国或监管机构根据《数据保护指令》第 26 条第 2 款所做的授权在被修改、替换或废止前仍然有效，必要的情况下由该监管机构变更。欧盟委员会根据《数据保护指令》第 26 条第 4 款所做的决定再被修改、替换或废止前也仍旧有效，如果必要的话，可以根据本条第 2 款以欧盟委员会决议的方式变更。

第四十七条 公司约束规则

1. 有权的监管机构应当按照第 63 条设置的一致性机制批准公司约束规则， 条件如下：

（a） 具有法律约束力，并且适用于企业集团有关的所有成员，或者参与到共同经济活动的企业团体，包括它们的雇员；

（b） 在处理数据主体的个人数据时明确授予他们可执行的权利；并且

（c） 履行第 2 款规定的要求。

2. 第 1 款规定的公司约束规则至少应当明确以下内容：

（a）企业集团或者参加到联合经济活动的企业团体以及它们中的每个成员的结构和联系方式；

（b） 单个数据转移或一系列的数据转移所涉及的个人数据的类别、处理的类型和目的、受影响的数据主体的类型以及第三国或其他国家的鉴定；

（c） 它的法律约束力的性质，包括对内和对外的性质；

（d） 统一数据保护原则的应用，尤其是目的限定，数据最小化，存储期限的限制，数据质量，数据系统保护和默认保护，处理的法律依据，处理特殊类型的个人数据，确保数据安全的措施，以及有关正在向不受公司约束规则限制的团体数据转移的要求；

（e） 数据主体在数据处理中的权利和行使这些权利的方法，包括有权不受自动处理决定的制约，也包括不受依据第 22 条识别分析的制约，数据主体还有权依据第 79 条在向成员国中有管辖权的法院起诉前先向有权的监管机构投诉， 并且有权获得救济，适当的时候还可以因对方违反公司约束规则获得赔偿金；

（f） 设立于欧盟成员国境内的数据控制者或数据处理者应承担其非设立于欧盟境内的分支违反公司约束规则所产生的责任；该数据控制者或数据处理者只有在证明该成员不应对造成损害的事件负责时能够全部或部分免除该项责任；

（g） 有关公司约束规则的内容，尤其是本款第(d)、(e)、(f)项规定的条款，如何按照本条例第 13 条和第 14 条的规定提供给数据主体；

（h） 每一个根据第 37 条指定的数据保护专员或者任何其他在企业集团或者参与到联合经济活动的企业团体内负责监督公司约束规则的遵守情况和培训以及投诉处理的人或机构的任务；

（i） 投诉的程序；

（j） 企业集团或者参与到联合经济活动的企业团体内部用来核实公司约束规则的遵守情况的机制，这些机制应当包括数据保护的审计，用来确保对数据主体权利的保护采取纠正措施的方法。核实的结果应当向(h)项中规定的个人或机构进行告知，同时也应告知企业集团或者参与到联合经济活动的企业团体的控制集团的董事会，并且在有权监管机构要求时能够及时

获取；

（k） 报告和记录规则变化的机制，并且将这些变化报告给监管机构；

（l） 与监管机构合作确保企业集团或者参与到联合经济活动的企业团体的每个成员都遵守规则的机制，尤其是确保监管机构知晓本款(j)项规定的审核措施的结果；

（m） 向有权监管机构和企业集团或者参与到联合经济活动的企业团体的成员报告所有法律要求的机制，当该成员是第三国的主体，并且该国很有可能会对公司约束规则提供的保证产生不利的影响时；

（n） 对于拥有定期和永久的个人数据访问权限的工作人员进行适当的数据保护培训。

3. 欧盟委员会可以为数据控制者、数据处理者和监管机构之间有关本条公司约束规则进行的信息交换制定相应的格式和程序。这些实施条例的制定应当符合本条例第 93 条第 2 款所规定的审查程序。

第四十八条 非经欧盟法律授权的转移和公开

第三国法院的任何判决或裁决以及行政机关的任何决定要求数据控制者或处理者转移或公开个人数据的，只能在请求的第三国与欧盟或成员国之间存在有效的国际协议的基础上才能被承认和执行，例如共同司法协助协议，并且不能损害根据本章节进行转移所需的其他条款。

第四十九条 特殊情形下的例外规定

1. 在缺乏本条例第 45 条第 3 款规定的充分保护标准或者缺乏本条例第 46 条规定的适当保护措施，包括公司约束规则在内时，将个人数据转移到第三国或国际组织应当满足以下条件之一：

（a）数据主体在被告知这种转移行为由于缺乏充分的保护标准和适当的保护措施可能会对其带来的风险后仍明确同意转移的；

（b） 转移是履行数据主体和数据控制者之间的合同义务或者是依据数据主体的要求履行的先合同义务所必要的；

（c）转移是数据控制者与其他自然人或法人订立和履行有关数据主体利益的合同的必要条件；

（d） 转移是为重要的公共利益所必要的；

（e） 转移是确立、行使或抗辩法定请求权的必要条件；

（f） 在数据主体由于生理上的或法律上的原因不能给予同意的情况下，转移是为保护数据主体或其他人的重要利益所必要的；

（g） 转移源自某登记簿，该登记簿是依据欧盟或者成员国的法律的规定为了向公众提供信息或者向不特定公众或证明存在合法利益的特定主体开放查询而设立的；欧盟或成员国法律规定的查询条件限于特定的案件需要。

当转移不能依据第 45 条或第 46 条包括公司约束规则在内的条款时，也不存在适用本款(a)至(g)项的特殊情形下的例外规定时，向第三国或国际组织转移个人数据只有在满足下面的条件时才能进行：转移没有重复进行，只关系到有限数量的数据主体，是为了数据控制者追求合法利益目的所必要的，并且该利益没有被数据主体的利益、权利和自由所覆盖，同时数据控制者已经围绕数据转移评估了所有的情形，并且根据该评估提供了保护个人数据的适当的措施。数据控制者应当将要进行的数据转移通知监管机构。数据控制者除了提供第 13 条和第 14 条规定的信息外，还应告知数据主体将要进行的数据转移和追求的合法利益。

2. 依据本条第 1 款(g)项的规定，转移不应包含登记簿中记载的个人数据的整体或个人数据的所有类别。当登记簿被提供给具有合法利益的人员查询时，只有依据其请求或其成为接收者时，才能进行转移。

3. 行政机构行使它们的公共职权时，第 1 款(a)、(b)、(c)项和第 1 款中的第 2 段不适用。

4. 本条第 1 款(d)项涉及的公共利益应当被欧盟法律及数据控制者所属的成员国法律所认可。

5. 在缺乏充分保护标准的情况下，出于公共利益的重要原因的考量，欧盟或成员国法律可以明确设置特殊类型个人数据转移到第三国或国际组织的限制。成员国应当将这类条款告知欧盟委员会。

数据控制者或处理者应当按照第 30 条的规定将本条第 1 款第 2 段规定的适合的安全保障措施和评估报告记录在档案中。

第五十条 个人数据保护的国际合作

当涉及第三国和国际组织时，欧盟委员会和监管机构应当采取下列适当措施：

（a） 建立国际合作机制来促进个人数据保护法律的有效实施；

（b） 在个人数据保护法律执法领域提供国际互助协作机制，包括通知转送、投诉提交、调查协助以及信息交换。该协助受个人数据保护措施和其他基础权利和自由保护的限制；

（c）邀请相关的利害关系人参与旨在改进个人数据保护法的实施的国际合作讨论会或活动；

（d） 加强有关个人数据保护的立法和实践上的交流和文档管理，包括与第三国的司法管辖权的冲突。

第六章 独立的监管机构

第一节 独立的地位

第五十一条 监管机构

1. 每个成员国应当安排一个或一个以上的独立的公共机构来负责监督本条例的实施，来保护在个人数据处理中涉及到的自然人的基础权利和自由，并促进个人数据在欧盟范围内的自由流通。（“监管机构”）

2. 每个监管机构应当致力于对于本条例在欧盟范围内的一致适用，为了实现这一目的，监管机构应当按照第七章的规定相互合作并且与委员会合作。

3. 当一个成员国内有多个监管机构设立的情形下，该成员国应当指定其中一个监管机构在欧洲数据保护委员会中代表这些机构，并且应当设立机制来确保其他机构对于与第 63 条规定的一致性机制的遵守。

4. 各成员国应当最迟在 2018 年 5 月 25 日前毫不迟延地通知欧盟委员会其依据本章内容自行制定的法律条款和对这些条款有影响力的后续修正案。

第五十二条 独立性

1. 每个监管机构在履行它们的任务和行使他们的权力时应当按照本条例的规定保持完全的独立。

2. 每个监管机构的成员在依照本条例执行他们的任务和行使他们的职权时应当保持不受外部的影响，不管是直接的还是间接的，也不应寻求或者接受任何人的指示。

3. 每个监管机构的成员应当停止任何与他们职责相冲突的行为，并且在他们的任职期间，不应参与任何相冲突的职业，不管获利与否。

4. 各成员国应当确保向监管机构提供人力、技术和财政资源、办公场所和必要的基础设施，来确保他们能够有效地履行职责，行使权力，包括在欧洲数据保护委员会的互助、合作和参与背景下才能实施的职责和权力。

5. 各成员国应当确保每个监管机构选择并拥有它们自身的职员，并且这些职员应当只听从监管机构成员的指示。

6. 各成员国应当确保每个监管机构都是其自身财政的控制主体，使得其独立性不受干扰，并且监管机构具有区分开的、公开的属于超越地方一级的或者国家级的年度预算。

第五十三条 监管机构成员的一般条件

1. 成员国应当保证每个监管机构的成员都能通过以下透明的方式来被任命:

-成员国议会;

-成员国政府;

-成员国国家元首；或者

-按照成员国的法律将任命权委托给一个独立的机构。

2. 每个成员需要具备履行他们职责和行使他们权力所需要的资质、经验和技能，尤其在保护个人数据领域。

3. 根据成员国相关法律的规定，监管机构成员的职责在其任期届满、辞职以及强制退休后终止。

4. 监管机构成员只能是在重大失误或者该成员不再满足履行职责所必须具备的条件时才能解雇。

第五十四条 设立监管机构的规则

1. 每个成员国应当在法律上规定所有以下内容:

（a） 每一监管机构的设立;

（b） 每个监管机构成员被任命所需的资质和资格条件;

（c） 任命每个监管机构成员的规则和程序;

（d） 监管机构成员的每届任期不得少于四年，除非是在 2016 年 5 月 24 日后进行的第一次任命，这使得部分成员的任期可能更短一些。因为交叉任命程序是保护监管机构独立性的必要条件;

（e） 是否存在以及如果存在则每个监管机构的成员需要经过几次任期才能有资格被重新任命;

（f） 管理监管机构成员或工作人员义务的条件，禁止的行为，职业和利益与在职期间或任期结束后有冲突的以及停止工作的管理规则。

2. 依照欧盟或成员国法律，考虑到在履行义务和行使职权的时候已经知悉了 机密信息，监管机构的成员和职员在任期内或任期结束后都是负有专业保密义务。在他们的任期内，职业

性保密义务尤其适用于自然人报告违反本条例的情形。

第二节 权限、职责与权力

第五十五条 权限(Competence)

1. 各监管机构应当依照本条例规定在各自所在成员国境内履行所分配的职责，行使所授予的权力。

2. 公共机构或私人主体依据本条例第 6 条第 1 款(c)或(e)项规定处理个人数据的，成员国的相关监管机构具有管理权限。本条例第 56 条的规定在这类案件中不再适用。

3. 监管机构无权监管法院行使司法职权所实施的数据处理操作。

第五十六条 主要监管机构的权限

1. 数据控制者或处理者跨境处理数据的，则其主要营业场所或单一营业场所的监管机构有权作为主要监管机构，并根据本条例第 60 条规定的程序监督该数据处理活动，但其监管行为不得违反本条例第 55 条的规定。

2. 如果处理行为只与监管机构所在成员国内的营业场所有关，或者只在监管机构所在成员国内对数据主体有实质性影响，各监管机构都有权处理向它提出的投诉或者可能违反条例的行为而无需遵循本条第 1 款的规定。

3. 在本条第 2 款规定的情形下，监管机构应毫不迟延地将事项告知主要监管机构。主要监管机构应当考虑数据控制者或处理者在通知它的监管机构所在成员国内是否有营业场所，并在被告知后的三周内决定是否根据本条例第 60 条规定的程序处理该案件。

4. 当主要监管机构决定处理案件时，应当适用本条例第 60 条规定的程序。向主要监管机构做出通知的监管机构可以针对主要监管机构的决定向其提交草案。主要监管机构在准备本条例第 60 条第 3 款规定的决定草案时，应当充分考虑该草案。

5. 当主要监管机构决定不处理该案件时，向主要监管机构做出通知的监管机构应当根据本条例第 61 条和第 62 条的规定处理案件。

6. 主要监管机构应当是进行跨境数据处理活动的数据控制者或处理者的唯一对话者。

第五十七条 职责

1. 在不影响本条例规定的其他职责的前提下，各监管机构应当在其领土范围内履行以下职责：

（a） 监督和促进本条例的适用；

（b） 提高公众对于个人数据处理相关的风险、规则、保障措施和权利的认知和理解。专门针对儿童的活动还应得到特别关注；

（c） 根据成员国法律，向国家议会、政府以及其他立法、行政机构、团体提供处理个人数据所涉及的保护自然人权利与自由的立法、行政措施的意见；

（d） 提高数据控制者和处理者对本条例所规定义务的认识；

（e） 依据请求向数据主体提供关于行使本条例所赋予权利的信息。必要时，可与其他成员国的监管机构合作以实现此目的；

（f） 依据本条例第 80 条的规定处理数据主体或团体、组织或协会提出的投诉，适当调查有关事项，并在合理期间内将处理投诉的进程和结果告知数据主体、团体、组织或协会，尤其在有必要进一步调查或与其他监管机构合作时；

（g） 为确保本条例适用、实施的一致性，与其他监管机构开展包括分享信息、相互提供帮助在内的合作；

（h） 开展关于本条例适用情况的调查，包括根据从其他监管机构或其他公共机构获得的信息；

（i） 关注会对个人数据保护产生影响的相关事物的发展，特别是信息和通信技术、商事惯例的发展；

（j） 推出本条例第 28 条第 8 款和第 46 条第 2 款(d)项规定的标准合同条款；

（k） 建立并保存一份关于本条例第 35 条第 4 款规定的评估数据保护影响评估的要求的清单；

（l） 对本条例第 36 条第 2 款规定的数据处理活动提供建议；

（m） 鼓励根据本条例第 40 条第 1 款的规定起草行为准则(codes of conduct)，并对根据本条例第 40 条第 5 款的规定起草的提供充分保护的“行为准则”提出意见并给予批准；

（n） 鼓励根据本条例第 42 条第 1 款的规定建立数据保护认证机制，以及数据保护印章和标记，并批准本条例第 42 条第 5 款规定的认证标准；

（o） 必要时，对根据本条例第 42 条第 7 款发放的认证实施定期审查；

（p） 起草并发布本条例第 41 条规定的监督行为准则实施的机构的认证标准、第 43 条规定的认证机构的认证标准；

（q） 实施本条例第 41 条规定的监督行为准则实施的机构和第 43 条规定的认证机构的认证；

（r） 授权合同条款和本条例第 46 条第 3 款规定的规定；

（s） 批准本条例第 47 条规定的公司约束规则；

（t） 协助欧洲数据保护委员会的活动；

（u） 对违反本条例的行为以及根据本条例第 58 条第 2 款采纳的措施进行内部记录；

（v） 履行关于个人数据保护的其他职责。

2. 各监管机构应当采取措施促使本条第 1 款(f)项规定的投诉的提交更加便利。例如，投诉的递交在不排除其他的通信方式的情况下可以以完全电子化的方式。

3. 监管机构履行职责时不应对数据主体、数据保护专员（如果有）收取费用。

4. 当数据主体的请求明显无根据或很过分，尤其是重复请求时，监管机构可以以行政成本为基础收取合理的费用或者对其提出的要求不予理睬。监管机构应承担请求明显无根据或很过分的证明责任。

第五十八条 权力

1. 各监管机构应当享有下列调查权力：

（a） 命令数据控制者或数据处理者、其代表人（如果有）提供其履行职责所必要的所有信息；

（b） 以数据保护审计的形式实施调查；

（c） 对根据本条例第 42 条第 7 款发放的认证实施审查；

（d） 通知数据控制者或者数据处理者其被认定违反了本条例；

（e） 从数据控制者和处理者处访问行使职责所必要的一切个人数据和信息；

（f） 进入数据控制者和处理者的经营场所，包括任何处理数据的设备与工具，行使该权力应当遵守欧盟或成员国的程序法。

2. 各监管机构应当享有下列矫正权力：

（a） 向欲实施的数据处理活动很可能违反本条例规定的数据控制者或处理者发出警告；

（b）向实施的数据处理活动违反了本条例的规定的数据控制者或处理者发出训斥；

（c）命令数据控制者或数据处理者遵从数据主体行使本条例赋予的权利的请求；

（d）命令数据控制者或数据处理者使其数据处理活动遵从本条例的规定，必要情况下要求其在指定的时期内以指定的方式实施；

（e）命令数据控制者向数据主体告知其个人数据的泄露情况；

（f）强加临时性或终局性的限制，包括数据处理的禁令；

（g）命令更正、消除违反本条例第 16、17、18 条规定的限制而处理的个人数据，并将此结果告知本条例第 17 条第 2 款和第 19 条规定获取数据的接收方；

（h）撤销认证，或者命令认证机构撤销根据本条例第 42、43 条发放的认证，或者命令认证机构对不能达到或不再达到认证标准的不予发放认证；

（i）处以本条例第 83 条规定的行政罚款，或根据个案实施本条规定以外的替代措施；

（j）命令暂停向第三国或国际组织的数据接收者转移数据。

3. 各监管机构应当享有下列授权和建议的权力：

（a）建议数据控制者遵循本条例第 36 条规定的事先征询程序；

（b）主动或者根据请求，根据成员国法律就有关个人数据保护的问题向国家议会、成员国政府或其他政治机构以及公众发表意见；

（c）如果成员国的法律需要事先授权，授权本条例第 36 条第 5 款规定的数据处理；

（d）对本条例第 40 条第 5 款规定的行为准则发表意见并作出批准；

（e）根据本条例第 43 条授权认证机构；

（f）根据本条例第 42 条第 5 款发放认证并批准认证标准；

（g）采用本条例第 28 条第 8 款和第 46 条第 2 款(d)项规定的标准数据保护条款；

（h）授权本条例第 46 条第 3 款规定的合同条款；

（i）授权本条例第 46 条第 3 款规定的行政安排；

（j）批准本条例第 47 条规定的公司约束规则。

4. 监管机构依据本条规定行使授予的权力应当受到合理的保护，包括列在欧盟和成员国法律中、符合宪章的有效的司法救济、正当程序。

5. 各成员国应当在法律上规定各监管机构享有将违反本条例的行为诉诸司法机构的权力，或在合适的情况下启动或参与其他法律程序，以强制实施本条例的规定。

6. 各成员国应当在法律上规定各监管机构享有其他在本条第 1、2、3 款中规定的权力。行使这些权力不能损害本条例第七章的有效实施。

第五十九条 工作报告

各监管机构应当就其工作起草年度报告，报告应包含被告知的违反条例的行为种类、根据本条例第 58 条第 2 款采纳的措施种类的清单。这些报告应呈交给国家议会、政府和其他成员国法律指定的机构，并向公众、欧盟委员会、欧洲数据保护委员会公开。

第七章 合作与一致性

第一节 合作

第六十条 主要监管机构和其他相关监管机构的合作

1. 主要监管机构与其他相关监管机构应当根据本条进行合作以努力达成共识。主要监管机构和相关监管机构应当互相交换所有的相关信息。

2. 主要监管机构可以根据本条例第 61 条在随时要求其他相关监管机构提供相互协助，可以根据本条例第 62 条开展联合行动，尤其在针对营业场所在其他成员国境内的数据控制者或处理者实施调查，或者监督措施的实施时。

3. 主要监管机构应当毫无延迟地将相关信息告知其他相关监管机构。它应当毫无延迟地向其他相关监管机构提交决定草案，咨询他们的意见，考虑他们的观点。

4. 任何其他相关监管机构在根据本条第 3 款被咨询后的四周内，对决定草案表示出相关且合理的反对意见，主要监管机构若不遵循该相关且合理的反对意见，或者认为该反对意见既不相关也不合理，则应将该案件提交到本条例第 63 条规定的一致性机制。

5. 主要监管机构若遵循该相关且合理的反对意见，则应当向其他相关监管机构提交修改后的决定草案并咨询他们的意见。修改后的决定草案应当适用本条第 4 款规定的程序，期限为两周。

6. 若其他相关监管机构在本条第 4、5 款规定的期限内未对主要监管机构提交的决定草案提出反对意见，应当认为主要监管机构和其他相关监管机构均同意该决定草案并受其约束。

7. 主要监管机构应当采纳决定并将决定告知案件涉及的数据控制者或处理者的主要营业场所或单一营业场所，视具体情况通知其他相关监管机构和欧洲数据保护委员会，告知内容应包括相关事实的简述以及依据。接到投诉的监管机构应当将决定告知投诉者。

8. 当投诉被驳回或者被反对，收到投诉的监管机构应当采纳决定并通知投诉者、数据控制者，无需遵循本条第 7 款的规定。

9. 当主要监管机构和相关监管机构同意驳回或反对部分投诉，回应其他部分的投诉，每个部分应独立作出决定。当主要监管机构作出有关数据控制者行动的决定，应当告知其成员国领土范围内的数据控制者或处理者的主要营业场所或单一营业场所，并告知投诉者。当主要监管机构作出有关驳回或反对投诉的决定，应当告知投诉者，并告知数据控制者或处理者。

10. 根据本条第 7 款和第 9 款的规定收到主要监管机构的通知后，数据控制者或处理者应当采取必要措施来确保在欧盟境内的所有营业场所的数据处理活动遵循该决定。数据控制者和处理者应当将为遵循决定所采取的措施告知主要监管机构以及其他相关监管机构。

11. 在例外情形下，当相关监管机构有理由认为有紧急必要性去采取行动以保护数据主体的利益时，应当适用本条例第 66 条规定的紧急程序。

12. 主要监管机构和其他相关监管机构应当通过电子形式，采用标准格式互相提供本条规定所要求的信息。

第六十一条 相互协助

1. 为了实现本条例在实施和适用上的一致性以及制定措施来使监管机构之间的合作更加有效，各监管机构应当互相提供相关信息并相互协助，相互协助的内容尤其应当包括信息要求、监督措施如实施事先授权和事先征询、检查和调查的要求。

2. 各监管机构应在不迟于收到请求后的一个月内采取所要求的适当措施来回应其他监管机构的请求。这些措施可以包括中止在调查过程中相关信息的转移行为。

3. 协助请求应包含请求的目的和理由在内的所有必要信息。信息交换仅用于其要求的目的。

4. 监管机构对所收到协助请求不得拒绝处理，除非有以下情况：

（a） 监管机构无权处理请求的事项或者无权采取请求实施的措施；

（b） 处理该请求会与监管机构所适用的本条例、欧盟及成员国的法律相矛盾。

5. 被请求的监管机构应当将请求处理的结果，或者视具体情况将为满足监管机构的请求而采取的措施的实施情况告知提出请求的监管机构。被请求的监管机构应当根据本条第 4 款规定为拒绝处理请求说明理由。

6. 通常，被请求的监管机构应将其他监管机构所要求的信息通过电子形式以标准格式提供给提出请求的监管机构。

7. 被请求的监管机构不得对基于相互协助请求而采取的行动收取费用。在例外情况中，监

管机构可以就相互协助条款中所产生具体支出的补偿达成共识。

8. 若监管机构在收到其他监管机构的请求后一个月内不提供本条第 5 款规定的信息，提出请求的监管机构可以依据本条例第 55 条第 1 款的规定在其所在成员国的领土范围内采取临时措施。在这种情况下，应当推定达到了实施本条例第 66 条第 1 款规定的紧急必要性，可以请求欧洲数据保护委员会根据本条例第 66 条第 2 款做出紧急的有约束力的决定。

9. 欧盟委员会可以具体规定本条涉及的相互协助的文本格式与程序，以及各监管机构之间、监管机构与欧洲数据保护委员会之间的信息交换安排，尤其是本条第 6 款规定的信息交流的标准格式。这些实施条款的制定应当符合本条例第 93 条第 2 款所规定的审查程序。

第六十二条 监管机构的联合行动

1. 监管机构应在合适的时候开展联合行动，包括联合调查、联合执行措施， 联合行动应有其他成员国监管机构的成员或职员的参与。

2. 当数据控制者或处理者在数个成员国有营业场所或者数据处理操作可能 实质影响数个成员国的多数数据主体时，这些成员国的监管机构都应参与联合行 动。根据本条例第 56 条第 1 款和第 4 款的规定有管辖权的监管机构应邀请这些成员国的监管机构参加联合行动，并毫无迟延地回应监管机构参与该行动的请求。

3. 监管机构可以依据成员国的法律、协助监管机构的授权赋予协助监管机构以权力，包括授予参与联合执法的协助监管机构的成员或职员以调查权，或者在主办监管机构所在国家法律允许的情形下，授权协助监管机构的成员或职员依据协助监管机构所在成员国的法律行使其调查权。协助监管机构只有在主办监管机构的成员或职员在场和指导下才能行使该调查权。协助监管机构的成员或职员应受主办监管机构国家法律的约束。

4. 当协助监管机构的职员根据本条第 1 款的规定在其他成员国参与行动，主办监管机构应当根据行动所在成员国的法律规定对他们的行为承担责任，包括对行动中他们造成的损害承担赔偿责任。

5. 发生损害的成员国应当按照其自己职员造成损害的情形赔偿此种损害。职员对其他成员国领土范围内的任何人造成损害的，协助监管机构所在成员国应当向权利人全额支付其有权获得的赔偿额。

6. 在不妨害相对第三人权利的行使的前提下，作为本条第 5 款规定的例外， 各成员国在本条第 1 款规定的情形下应当避免就本条第 4 款规定的损害向其他成员国要求赔偿。

7. 当计划开展联合行动，而某监管机构未在一个月内履行本条第 2 款第 2 句规定的义务时，其他监管机构应有权依据本条例第 55 条的规定在其所在成员国的领土范围内采取临时性措施。在该情形下，应当推定达到了本条例第 66 条第 1 款规定的采取措施的紧急必要性，可以根据本条例第 66 条第 2 款的规定向欧洲数据保护委员会请求意见或者紧急有约束力的决定。

第二节 一致性

第六十三条 一致性机制

为了本条例在欧盟境内的统一适用，各监管机构应依据本节规定的一致性机制开展相互合作，或与欧盟委员会合作。

第六十四条 欧洲数据保护委员会的意见

1. 当有权限的监管机构将采取以下措施时，欧洲数据保护委员会应当提出意见。为达到该目的，当有下列情形，监管机构应向欧洲数据保护委员会(the European Data Protection Board)①传达决定草案：

（1 ）为强化欧盟数据保护的协作程度，根据《统一数据保护条例》将新设 the European Data Protection Board (EDPB) ，该委员会将取代"第 29 条数据保护工作组"(the Article 29 DP Working Party，该工作组是根据 1995 年数据保护指令设立的，每个成员国的数据保护监管机构在工作组中有一个席位)成为常设机构。关于该委员会的规定参见第 68 至 76 条。

（a）针对依据本条例第 35 条第 4 款的规定需要达到数据保护影响评估要求的一系列处理操作行为；

（b）关于依据本条例第 40 条第 7 款的规定，行为准则草案或修正案或行为准则的扩展是否符合本条例规定；

（c）针对本条例第 4 条第 3 款规定的机构或者第 43 条第 3 款规定的认证机构的认证标准的批准；

（d）针对本条例第 46 条第 2 款(d)项和第 28 条第 8 款规定的标准数据保护条款的决定；

（e）针对本条例第 46 条第 3 款(a)项规定的合同条款的认可；

（f）针对本条例第 47 条规定的公司约束规则的批准。

2. 任何监管机构、欧洲数据保护委员会和欧盟委员会的主席可以要求欧洲数据保护委员会对任何关于统一适用的情况或对多个成员国产生的影响进行调查以期获取意见，特别是当有权限的监管机构不遵循本条例进行第 61 条规定的相互协助或者第 62 条规定的联合行动。

3. 在本条第 1 款和第 2 款规定的情形下，欧洲数据保护委员会应当对向它提交的事项提出意见，如果它还未就同一问题提出过意见。该意见应当在八周内， 由欧洲数据保护委员会的简单多数成员通过后被采纳。考虑到事项的复杂性，该 期限可以延长六周。关于本条第 1 款规定的决定草案应当根据本条第 5 款的规定在欧洲数据保护委员会的成员中传阅，成员在主席指定的合理期限内没有反对的， 应当推定已经就该决定草案达成一致。

4. 监管机构和欧盟委员会应当通过电子形式以标准格式将任何相关信息提供给欧洲数据保

护委员会，包括视具体情况而定的事实概述、决定草案、有必要通过该措施的依据、其他相关监管机构的观点，不得无故拖延。

5. 欧洲数据保护委员会的主席应通过电子形式通知以下事项，不得无故拖延：

（a）将任何提供给它的相关信息以标准格式告知欧洲数据保护委员会和欧 盟委员会的成员。欧洲数据保护委员会的秘书应当在必要时提供相关信息的翻译；

（b）视具体情况，将意见告知本条第 1 款和第 2 款规定的监管机构和欧盟委员会，并将意见公开。

6. 有权限的监管机构不应在本条第 3 款规定的期限内采纳本条第 1 款规定的措施草案。

7. 本条第 1 款规定的监管机构应当充分考虑欧洲数据委员会的意见，并在收到意见后的两周内，以电子形式告知欧洲数据保护委员会的主席是否保持或修改决定草案，如果修改决定草案，需使用标准格式。

8. 相关监管机构在本条第 7 款规定的期限内通知数据保护委员会的主席其不会遵循数据保护委员会的所有或部分意见，并提供相关依据，此时应当适用本条例第 65 条第 1 款的规定。

第六十五条 欧洲数据保护委员会解决纠纷

1. 为了确保本条例在个案中正确且统一的适用，欧洲数据保护委员会应当在下列情形中作出有约束力的决定：

（a） 在本条例第 60 条第 4 款规定的情形下，相关监管机构对决定草案提出相关且合理的反对意见或者主要监管机构不认同该反对意见，认为其既不相关也不合理。有约束力的决定应当关注所有相关且合理的反对意见针对的事项，尤其是是否违反本条例的规定；

（b） 对哪一个相关监管机构对主要营业场所有管辖权有争议；

（c） 有管辖权的监管机构在本条例第 64 条第 1 款规定的情形下不向欧洲数据保护委员会寻求意见，或者在本条例第 64 条规定的情形下不遵循欧洲数据保护委员会的意见。在这种情况下，任何相关监管机构或者欧盟委员会可以将情况告知欧洲数据保护委员会。

2. 本条第 1 款规定的决定应当在提及主要情况后的一个月内，由欧洲数据保护委员会 2/3 多数的成员通过后作出。考虑到事项的复杂性，该期限可以延长一个月。本条第 1 款规定的决定应当被传达给主要监管机构和所有的相关监管机构， 并应向它们说明理由，这些监管机构受决定的约束。

3. 当欧洲数据保护委员会不能够在本条第 2 款规定的期限内作出决定，应当在本条第 2 款规定的第二个月届期后的两周内，由欧洲数据保护委员会的简单多数成员通过后采纳决定。当欧洲数据保护委员会的成员意见分离时，由主席投票决定是否采纳决定。

4. 相关监管机构不应在本条第 2、3 款规定的期限内就本条第 1 款规定的关于提交给欧洲数据保护委员会的事项作出决定。

5. 欧洲数据保护委员会的主席应当将本条第 1 款规定的决定告知相关监管机构，不得无故拖延。它也应当通知欧盟委员会。在监管机构已经通知了本条第 6 款规定的最终决定后，该决定应当被毫无延迟地发布在欧洲数据保护委员会的网站上。

6. 视具体情况，主要监管机构或者收到投诉的监管机构，应当在本条第 1 款规定的决定的基础上，最迟在欧洲数据保护委员会通知其决定后的一个月内作出最终决定，不得无故拖延。视具体情况，主要监管机构或者收到投诉的监管机构，应当在将最终决定分别告知了数据控制者或处理者和数据主体之后，将数据告知欧洲数据保护委员会。相关监管机构的最终决定应当根据本条例第 60 条第 7、8、9 款的规定作出。最终决定应当关于本条第 1 款规定的决定，应当详细说明第 1 款中的决定，将根据本条第 5 款的规定被公布在欧洲数据保护委员会的网站上。最终决定应附上本条第 1 款规定的决定。

第六十六条 紧急程序

1. 在例外情况下，相关监管机构可以不经本条例第 63、64、65 条规定的一致性机制，或者第 60 条规定的程序，在指定有效期内（不超过 3 个月）立刻采取临时措施以在其领土范围内产生法律效力。其条件是：当监管机构认为需要采取紧急措施以保护数据主体的权利和自由，监管机构应毫无迟延地将这些措施以及将他们适用于其他相关监管机构的理由告知欧盟委员会和欧洲数据保护委员会。

2. 当监管机构依据本条第 1 款的规定采取措施并认为最后措施需要被紧急采用时，它可以请求欧洲数据保护委员会给出紧急意见或紧急有约束力的决定。在请求紧急意见或紧急有约束力的决定时应当说明请求的理由。

3. 当有权监管机构在需要采取紧急措施却未采取适当措施时，任何监管机构可以请求欧洲数据保护委员会给出紧急意见或紧急有约束力的决定以保护数据 主体的权利和自由。在请求紧急意见或紧急有约束力的决定时应说明请求的理由， 包括行动的紧急必要性。

4. 无需遵守本条例第 64 条第 3 款和第 65 条第 2 款的规定，本条第 2、3 款规定的紧急意见或紧急有约束力的决定应被欧洲数据保护委员会的成员以简单多数的表决方式在两周内采纳。

第六十七条 交换信息

欧盟委员会可以采用通用的实施法令，为监管机构之间，监管机构和欧盟委员会之间通过本条例第 64 条规定的电子形式、特别是用标准格式进行信息交换列举安排。

这些实施法令的采用应当符合本条例第 93 条第 2 款规定的检验程序。

第三节 欧洲数据保护委员会

第六十八条 欧洲数据保护委员会(European Data Protection Board)

1. 欧洲数据保护委员会作为欧盟的机构由此设立，并应当具备独立人格。

2. 欧洲数据保护委员会应当由其主席代表。

3. 欧洲数据保护委员会应由每个成员国的监管机构负责人和欧洲数据保护监督员（the European Data Protection Supervisor）或者他们的代表人组成。

4. 当某个成员国有一个以上的监管机构负责监管本条例的适用时，应根据该成员国的法律提名一个联合代表人。

5. 欧盟委员会有权参与欧洲数据保护委员会的活动和会议，但不享有投票权， 并应当指派一名代表人。欧洲数据保护委员会的主席应将欧洲数据保护委员会的 所有活动向欧盟委员会报告。

6. 在本条例第 65 条规定的情形下，欧洲数据保护监督员只对关于欧盟的机构、组织、办公室、代办处适用的原则和规则的决定享有投票权，这实质上符合条例的规定。

第六十九条 独立性

1. 欧洲数据保护委员会依据本条例第 70 条、第 71 条的规定，在执行任务或行使权力时应独立活动。

2. 欧洲数据保护委员会在执行任务或行使权力时，不应寻求或采纳任何人的指示。该项规定并不影响对本条例第 70 条第 1 款(b)项和第 2 款规定的欧盟委员会要求的执行。

第七十条 欧洲数据保护委员会的任务

1. 欧洲数据保护委员会应确保本条例得到统一地适用。为此目的，欧洲数据保护委员会应自发或者依据欧盟委员会的相关要求履行以下义务:

（a） 不得违反国家监管机构的职责，在本条例第 64 条和第 65 条规定的情形下监督并确保本条例的正确实施;

（b） 就欧盟个人数据保护的任何问题向欧盟委员会提出建议，包括本条例的任何修正议案;

（c） 向欧盟委员会寻求关于数据控制者、处理者、监管机构之间交换信息的格式和程序的建议，寻求公司约束规则的建议;

（d） 提出清除本条例第 17 条第 2 款规定的从公共通信服务中获取的个人数据的链接、副本、复制件的指南、建议和最佳操作方式;

（e） 自发或者依据各成员或者欧盟委员会的要求检查关于本条例适用情况的任何问题并提出指南、建议和最佳操作方式，以促进本条例得到一致地适用；

（f） 根据本款(e)项的规定提出指南、建议和最佳操作方式的标准和依据本条例第 22 条第 2 款规定的基于识别分析决定的条件；

（g） 根据本款(e)项的规定提出关于泄露个人数据、本条例第 33 条第 1 款和第 2 款规定的无故拖延决定、数据控制者或处理者被要求通知个人数据泄露情况的指南、建议和最佳操作方式；

（h） 当个人数据泄露可能对本条例第 34 条第 1 款规定的自然人的权利和自由造成巨大威胁时，根据本款(e)项的规定提出指南、建议和最佳操作方式；

（i） 根据本款(e)项的规定提出指南、建议和最佳操作方式，以详细说明在数据控制者和处理者遵循公司约束规则的基础上的个人数据转移的标准和要求，以及本条例第 47 条规定的确保数据主体的个人数据保护的必要要求；

（j） 根据本款(e)项的规定提出指南、建议和最佳操作方式,以在本条例第 49 条第 1 款规定的基础上，详细说明个人数据转移的标准和要求；

（k） 起草关于监管机构适用本条例第 58 条第 1、2、3 款规定的措施、修改本条例第 83 条规定的行政罚款的指南；

（l） 审核本款(b)项规定的指南、建议和最佳操作规则的实际适用；

（m） 根据本款(e)项的规定提出指南、建议和最佳操作方式，根据第 54 条第 2 款之规定为自然人报告条例违反情况建立一般程序；

（n） 鼓励根据本条例第 40 条和第 42 条的规定起草行为准则，建立数据保护的认证机制、数据保护的印章和标记；

（o） 实施认证机构的认证，并根据本条例第 43 条的规定定期审查，并根据本条例 43 条第 6 款、第 42 条第 7 款的规定对认证机构、经许可的在第三国营业的数据控制者或处理者进行持续公共注册；

（p） 着眼于本条例第 42 条规定的认证机构的认证，规定本条例第 43 条第 3 款规定的要求；

（q） 向欧盟委员会提供关于本条例第 43 条第 8 款规定的认证要求的意见；

（r） 向欧盟委员会提供关于本条例第 12 条第 7 款规定的标记的意见；

（s） 向欧盟委员会提供关于第三国或国际组织的数据保护水平的充分性的评估意见，包括

第三国、某地区、该第三国内一个或多个指定区域、国际组织是否再也无法确保充分的数据保护水平。为达到该目的，欧盟委员会应当向欧洲数据保护委员会提供所有必要的文件，包括与第三国政府之间关于该第三国、某地区、指定区域或国际组织的通信；

（t）依据本条例第 64 条第 1 款规定的一致性机制对监管机构根据第 64 条第 2 款提交的决定草案提出意见；并对根据第 65 条规定提出有约束力的决定， 包括第 66 条规定的情况提出意见；

（u） 促进监管机构之间的合作和有效的双边或多边信息交换；

（v） 促进监管机构之间，适当条件下监管机构与第三国或国际组织的监管机构之间开展的共同训练项目和人员交流；

（w） 促进世界范围内的数据保护监管机构之间有关个人数据保护的知识、立法文件和操作准则的交流；

（x） 提供关于本条例第 40 条第 9 款规定的以欧盟等级起草的行为准则的意见；

（y）对监管机构和法院关于在一致性机制中处理的问题所采取的决定进行可公共访问的电子注册。

2. 在请求欧洲数据保护委员会给出意见时，欧盟委员会可以依据事情的紧急程度明确欧洲数据保护委员会提供意见的期限。

3. 欧洲数据保护委员会应向欧盟委员会和本条例第 93 条规定的委员会提出意见、指南、建议和最佳操作方式，并将其公开。

4. 欧洲数据保护委员会应当在合适时，与利益相关主体商议，给予他们在合理期限内发表意见的机会。欧洲数据保护委员会应当将商议程序的结果公开，不得违反本条例第 76 条的规定。

第七十一条 报告

1. 欧洲数据保护委员会应当起草欧盟、第三国和国际组织个人数据处理中自然人保护情况的年度报告。这份报告应公开并送达给欧盟议会、理事会和欧盟委员会。

2. 该报告应包括对本条例第 70 条第 1 款(l)项规定的指南、建议和最佳操作方式的实践情况以及第 65 条规定的有约束力的决定的评价。

第七十二条 程序

1. 欧洲数据保护委员会做出的决定应由其成员的简单多数表决通过，除非本条例有其他规定。

2. 欧洲数据保护委员会应以其成员 2/3 多数决制定其自己的程序规则并组织其日常运营的安排。

第七十三条 主席

1. 欧洲数据保护委员会应通过简单多数决从其成员中选出一个主席和两个副主席。

2. 主席和副主席的职务任期应当是五年，可以连选连任。

第七十四条 主席的任务

1. 主席有以下任务:

（a） 召集欧洲数据保护委员会的会议并准备议程;

（b） 将欧洲数据保护委员会根据第 65 条的规定采纳的决定告知主要监管机构和相关监管机构;

（c） 确保欧洲数据保护委员会及时完成任务，特别是关于第 63 条规定的一致性机制。

2. 欧洲数据保护委员会应在其程序规则下规定主席与副主席之间的任务分工。

第七十五条 秘书处

1. 委员会应当设立一个秘书处，该秘书处设在欧洲数据保护监管机构。

2. 秘书处应当仅凭委员会主席的指导执行任务。

3. 负责执行委员会根据本条例的规定授予任务的欧洲数据保护监管机构职员应区别于负责执行由欧盟数据保护监管机构授予任务的职员，前者须进行单独汇报。

4. 在适当情况下，委员会和欧盟数据保护监管机构应当制定并发布一份关于本条规定实施以及双方合作条款确定的解释备忘录，该备忘录适用于负责执行委员会根据本条例授予任务的欧盟数据保护监管机构职员。

5. 秘书处应当为委员会提供分析、行政管理和后勤保障支持。

6.秘书处主要负责以下事务:

（a） 委员会的日常事务;

（b） 委员会成员之间、委员会主席和欧盟委员会之间的沟通;

（c） 与其他机构和社会公众之间的沟通;

（d） 使用电子手段进行国内外通信；

（e） 相关信息的翻译；

（f） 委员会会议的前期准备与后续工作；

（g） 准备、起草和发布委员会通过的意见、关于解决监管机构之间争议的决定和委员会采用的其他文本。

第七十六条 保密工作

1. 在委员会认为有必要的情况下，依据程序规则应当对其讨论内容进行保密。

2. 对提交给委员会委员、专家及第三方代表的文件的访问应当遵守欧盟议会和理事会发布的《有关欧盟议会、理事会与委员会文件的公众访问的条例》[Regulation(EC)No 1049/2001]的规定。

第八章 救济方式、责任与制裁

第七十七条 向监管机构投诉的权利(Right to lodge a complaint with a supervisory authority)

1. 如果该数据主体认为涉及自身的个人数据处理行为违反了本条例的规定， 在不影响获得其他行政或司法救济的情况下，每一个数据主体都享有向监管机构 投诉的权利，尤其是在他或她惯常居所地、工作地或侵权行为主张地所属成员国 内投诉。

2. 接受投诉的数据监管机构应当告知投诉者关于该投诉的进展和结果，包括根据第 78 条获得司法救济的可能性。

第七十八条 针对监管机构的有效司法救济权(Right to an effective judicial remedy against a supervisory authority)

1. 在不影响获得其他行政或非司法救济的情况下，每一个自然人或者法人有权就监管机构对其做出的具有法律约束力的决定寻求有效的司法救济。

2. 在不影响获得其他行政或非司法救济的情况下，当第 55 条和第 56 条规定的主管监管机构并未处理投诉或者按照第 77 条的规定在三个月内未告知数据主体该投诉的进展与结果时，每一个数据主体都有权寻求有效的司法救济。

3. 针对监管机构的诉讼，应当向该监管机构设立地所在成员国的法院提起。

4. 当就监管机构的一项决定提起诉讼，且该决定系根据一致性机制优先于委员会的意见或

决定的，监管机构应当将该意见或决定提交给法院。

第七十九条 针对数据控制者或数据处理者的有效司法救济权(Right to an effective judicial remedy against a controller or processor)

1. 在不影响获得行政或非司法救济的情况下（包括本条例第 77 条规定的向监管机构提出投诉的权利），每一个数据主体在认为他或她基于本条例而享有的权利因为违反本条例规定的个人数据处理行为而遭受侵害时，均有权寻求有效的司法救济。

2. 针对数据控制者或数据处理者的诉讼，应当向该数据控制者或数据处理者营业场所所在成员国的法院提起。除此之外，也可以向该数据主体惯常居所地所在成员国的法院起诉，除非数据控制者或处理者是某成员国行使公权力的公共机构。

第八十条 数据主体代表(Representation of data subjects)

1. 对按照成员国国内法依法设立的、以公共利益为法定目标并且活跃于保护数据主体权利与自由领域的非营利性机构、组织或协会，数据主体有权委托其代表自己提出投诉、行使第 77、78 和 79 条赋予的权利以及第 82 条赋予的接受赔偿的权利。

2. 成员国可以规定，本条第 1 款规定的机构、组织或协会如果认为数据主体基于本条例而享有的权利因为个人数据处理行为而遭受侵害的，其有权不经数据主体授权依照第 77 条规定向该成员国有权监管机构提出投诉，并且行使第 78、79 条所赋予的权利。

第八十一条 诉讼中止(Suspension of proceedings)

1. 当有管辖权的成员国法院得知另一成员国的法院正在审理以同一数据控制者或处理者数据处理行为主题的诉讼时，该管辖法院应联系另一成员国的法院确认上述诉讼的存在。

2. 在另一成员国的法院正在审理以同一数据控制者或处理者数据处理行为为主题的诉讼时，除了最先受理的法院之外的任何有管辖权的法院都必须中止其诉讼程序。

3. 当这些诉讼程序在初审中都悬而未决时，如果最先受理的法院对该争议纠纷享有司法管辖权且其所适用的法律允许进行合并审理的，任何除了最先受理法院之外的法院也可以根据当事人一方的申请拒绝司法管辖权。

第八十二条 获得赔偿的权利(Right to compensation and liability)

1. 任何因为违反本条例的行为而遭受财产性或非财产性损失的人，都有权就所遭受的损失获得数据控制者或者数据处理者的赔偿。

2. 违反本条例规定的数据处理所涉及的数据控制者都应当对所造成的损失承担责任。数据处理者只对其未遵守本条例规定的特别针对处理者的义务或者其超越数据控制者的合法（lawful）指示或作出与该指示相反的行为造成的损失承担责任。

3. 如果能够证明数据控制者或处理者对导致损失发生的事件不负有任何责任，则应当免除其上述第 2 款规定的责任。

4. 当同一处理过程涉及多个数据控制者或数据处理者，或者仅涉及一个数据控制者和一个处理者，并且根据第 2 款和第 3 款的规定他们对处理造成的所有损失承担责任时，每个数据控制者或处理者都应当对全部损失承担责任，以确保数据主体获得有效的赔偿。

5. 数据控制者或处理者根据第 4 款规定支付了全部的损失赔偿金后，有权依照第 2 款规定的条件向其他涉事数据控制者或处理者主张追偿，要求他们对各自造成的损害部分承担相应的赔偿责任。

6. 企图通过诉讼程序实现获得赔偿的权利的，应向第 79 条第 2 款规定的成员国法律授权的管辖法院提起诉讼。

第八十三条 施加行政罚款的一般条件(General conditions for imposing administrative fines)

1. 每个监管机构应当确保在每个个案中根据本条规定对违反本条例第 4、5 和 6 款规定的违法行为所处以的行政罚款是有效、适当且具有告诫性的。

2. 应当根据个案的情况在采取第 58 条第 2 款(a)至(h)项和(j)项的措施的同时附加罚款或者是将其作为上述措施的替代。在个案中决定是否处以行政罚款以及罚款的数额时应当注意以下因素：

（a） 违法行为的性质、严重性和持续时间，考虑所涉处理的性质、范围或目的，以及受影响的数据主体的数量与其遭受损失的程度；

（b） 违法行为是基于故意还是过失；

（c） 数据控制者或处理者为减轻数据主体遭受的损失而采取的任何措施；

（d） 数据控制者或处理者的责任轻重程度，考虑其根据第 25 条和第 32 条实施的技术和组织性措施；

（e） 数据控制者或处理者此前是否有过任何相关的违法行为；

（f） 为纠正违法行为和减轻违法行为可能会带来的不利影响，与监管机构的合作程度；

（g） 受违法行为影响的个人数据的种类；

（h） 监管机构获知违法行为的方式，尤其是数据控制者或处理者是否主动告知违法行为，以及如果是，则其告知到了何种程度；

（i） 如果之前就已经因相同事项对数据控制者或处理者采取了第 58 条第 2 款的措施，这

些措施的遵守情况如何；

（j） 对第 40 条规定所认可的行为准则或第 42 条规定所认可的认证机制的遵守情况；

（k） 任何其他适用于该个案情形的加重或减轻情节，例如直接或间接地通过违法行为所获得的经济利益或所避免的损失。

3. 如果数据控制者或处理者故意地或过失地基于相同的或相关的处理操作， 违反了本条例的多条规定对其施加的行政罚款的总数不得超过最严重违法行为的特定数额。

4. 违反以下规定，应当按照本条第 2 款的规定处以 10,000,000 欧元的行政罚款，或相对人是企业时则处以其上一财政年度全球营业总额 2%的行政罚款， 二者竞合取较高者：

（a）第 8、11、25、26、27、28、29、30、31、32、33、34、35、36、37、38、39、42 和 43 条规定的数据控制者和处理者的义务；

（b） 第 42 条和第 43 条规定的认证机构的义务；

（c） 第 41 条第 4 款规定的监管机构的义务。

5. 违反以下规定，应当按照本条第 2 款的规定，处以 20000000 欧元的行政罚款，或相对人是企业时则处以其上一财政年度全球营业总额 4%的行政罚款， 二者竞合取较高者：

（a） 第 5、6、7 和 9 条规定的数据处理的基本原则，包括同意的条件；

（b） 第 12 到 22 条规定的数据主体的权利；

（c） 第 44 到 49 条中对向第三国或国际组织转移个人数据的规定；

（d） 根据第九章的规定正式通过的成员国法律所规定的义务；

（e） 未遵守监管机构根据第 58 条第 2 款的规定所作出暂停数据流动的命令或者临时或最终的处理限制，或违反第 58 条第 1 款的规定未提供访问。

6. 未遵守监管机构根据第 58 条第 2 款规定所作出命令的，按照本条第 2 款的规定，应当被处以 20000000 欧元的行政罚款，或相对人是企业则处以其上一财政年度全球营业总额 4%的行政罚款，二者竞合取较高者。

7. 在不影响第 58 条第 2 款规定的监管机构纠正权的情形下，每个成员国可以就是否对其国内的政府机关和公共机构处以行政罚款以及处罚程序制定各自的规则。

8. 监管机构根据本条的规定行使其权力时应当遵守欧盟法和成员国法律规定的适当法律程序，包括有效的司法救济和正当程序规则。

9. 当成员国的法律体系没有规定行政罚款时，可以通过由有权监管机构提出罚款再由有管辖权的国内法院予以执行的方式适用本条规定，同时确保这些法律救济是有效的并且与监管机构所处的行政罚款有同等的效果。在任何情况下，所处罚款应当是有效的、适当的并且具有告诫性。上述成员国应在 2018 年 5 月 25 日前毫不迟延地告知委员会其依据本款制定的法律规定和一切后续的修正案。

第八十四条 处罚(Penalties)

1. 成员国应当针对违反本条例规定的行为尤其是不服从于第 83 条规定的行政性罚款的违法行为制定其他形式的处罚，并且应当采取所有必要的措施确保该处罚的执行。该处罚必须是有效的、适当的并且具有告诫性。

2. 每个成员国应在 2018 年 5 月 25 日前毫不迟延地告知委员会其依据第 1 款制定的法律规定和一切后续的修正案。

第九章 有关特殊数据处理情形的规定

第八十五条 数据处理与表达和信息自由

1. 成员国应当在法律上协调本法规定的个人数据保护权利与表达和信息自由权利的关系，包括基于新闻事业目的和学术、艺术或文学表达目的的数据处理。

2. 当数据处理是出于新闻事业目的或者学术、艺术、文学表达的目的，如果协调个人数据保护的权利与表达、信息自由关系是必要的，成员国应当提供对以下规定的豁免和克减：第二章原则、第三章数据主体的权利、第四章数据控制者和处理者、第五章向第三国或国际组织转移个人数据、第六章独立的监管机构、第七章合作与一致性、第九章有关特殊数据处理情形的规定。

3. 每个成员国应当将其依照本条第 2 款制定的法律条款和任何后续修正案毫不迟延地告知欧盟委员会。

第八十六条 对官方文件的公共访问与处理(processing and public access to official documents)

为了协调公众访问官方文件和本条例规定的个人数据保护的权利，由公共权力机关、公共团体或执行公共利益任务的私人团体掌握的官方文件中的个人数据可以被符合欧盟和成员国法律规定的机关或团体披露。

第八十七条 国民身份证号码的处理

成员国可以进一步确定国民身份证号码或其他任何通常应用识别符处理的特定情形。在这种情况下，国民身份证号码或其他任何通用的识别符只能在依照本条例规定数据主体的权利和自由获得适当保护的情形下使用。

第八十八条 人事领域的数据处理

1. 成员国可以在法律上或在集体协议中规定更加明确的规则，确保在人事领域处理员工个人数据时其权利和自由能够获得保护，特别是为了招聘、履行劳动合同，包括在法律上和在集体协议中确立的义务履行、经营管理、计划和组织工作、工作场所的平等和多样性、工作中的健康和安全、员工和客户财产的保护； 或者是为了个人或集体行使和享有雇员的权利和利益；或者为了雇佣关系终止的目的。

2. 这些规则应当包括合适和特定的措施以保护数据主体的人格尊严、合法利益和基本权利，特别是关于处理的透明性，企业集团内的个人数据的转移，或者参与联合经济活动和在工作场所从事系统监测的企业。

3. 每个成员国应当在 2018 年 5 月 25 日前将其依据本条第 1 款制定的法律条款及后续的修正案毫不迟延地告知欧盟委员会。

第八十九条 对基于公共利益存档目的、科学或历史研究目的、统计目的的数据处理的保护和克减(derogations)

1. 为了保护数据主体的权利和自由，根据本条例的规定，基于公共利益存档目的、科学或历史研究目的、统计目的而进行的个人数据处理行为应当采取适当的保护措施。这些保护应确保技术和组织措施到位，特别是为了确保遵守数据最小化原则。假如这些目的可以通过其他的方式实现，这些措施可以包括假名化机制。当这些目的可以通过不允许或不再允许对数据主体进行身份识别的深度处理方式实现时，这些目的将通过该方式得以实现。

2. 当为科学或历史研究目的、统计目的进行个人数据处理时，欧盟或成员国法律可以针对第 15、16、18 和 21 条规定的权利和本条第 1 款规定的安全保护措施设定克减条款，当上述这些权利可能对特定目的的实现产生不可想象或严重的损害，则该克减对目的的实现是必不可少的。

3. 当个人数据因公共利益存档目的被处理时，欧盟法律或成员国法律可以针对第 15、16、18、19、20 和 21 条规定的条件和本条第 1 款规定的安全保护措施设定克减条款，当上述这些权利可能对特定目的的实现产生不可想象或严重的损害，则该克减对目的的实现是必不可少的。

4. 当根据第 2 款和第 3 款的规定个人数据处理同时用于其他目的时，克减条款应当仅适用于本条规定的目的。

第九十条 保密义务(Obligations of secrecy)

1. 成员国可以制定法律，依照本条例第 58 条第 1 款(e)和(f)项规定列明监管机构对数据控制者和处理者的权力。鉴于数据控制者和数据处理者是各主权国家的法律或有权机构所制定的规章所规定的职业保密义务或其他相当的保密义务的义务主体，这样的规范对于平衡个人数据保护权利和保密义务的关系是必要且适当的。上述规则仅适用于数据控制者或数据处理

者从负有保密义务的活动中收到的或获取到的个人数据。

2. 每个成员国应在 2018 年 5 月 25 日前毫不迟延地告知委员会其依据本条第 1 款制定的法律规定和一切后续的修正案。

第九十一条 教会和宗教团体的现有数据保护规则

1. 若某个成员国的教会、宗教团体或社团在本条例生效之时已经在数据处理中适用全面保护自然人的综合性规则，那么只要该规则与本条例内容一致，该规则即可继续适用。

考虑到要实现本条例第六章规定的条件，适用本条第 1 款的综合性规则的教会和宗教团体应当受到独立监管机构的监管。

第十章 授权性法令与实施性法令

第九十二条 实施授权(Exercise of the delegation)

1. 授予欧盟委员会通过授权性法令的权力受本条规定的条件约束。

2. 本条例第 12 条第 8 款和第 43 条第 8 款授予欧盟委员会的委托权力自 2016 年 5 月 24 日起生效，期限不确定。

3. 欧盟议会或理事会可以随时撤销本条例第 12 条第 8 款和第 43 条第 8 款授予欧盟委员会的委托权力。撤销决定可以终止之前的决定中授予的权力。该决定自在欧盟官方公报发表之日的次日或者在此之后的一个指定日期生效。该决定不会影响任何已生效实施的授权性法令的效力。

4. 欧盟委员会一经通过授权性法令即应同时通知欧盟议会和理事会。

5. 欧盟委员会依据本条例第 12 条第 8 款和第 43 条第 8 款通过的授权性法令仅在欧盟议会或者理事会在收到相关法律后三个月内不表示反对，或者是在该期间届满前欧盟议会和理事会均告知欧盟委员会其不反对该法律的情形下，才正式生效。若欧盟议会或理事会提议，该期间可再延长三个月。

第九十三条 委员会程序

1. 欧盟委员会应由一个委员会辅助。该委员会具有《制定有关各成员国控制欧盟委员会行使执行权的控制机制的一般规则与原则的条例》[Regulation（EU）182/2011]所规定的委员会地位。

2. 本款参见《制定有关各成员国控制欧盟委员会行使执行权的控制机制的一般规则与原则的条例》[Regulation（EU）182/2011]第 5 条的规定。

3. 本款参见《制定有关各成员国控制欧盟委员会行使执行权的控制机制的一般规则与原则

的条例》[Regulation（EU）182/2011]第 5 条和第 8 条的规定。

第十一章 最终条款

第九十四条 《数据保护指令》(Directive 95/46/EC)的废止

1. 《数据保护指令》(Directive 95/46/EC）自 2018 年 5 月 25 日起废止。

2. 凡是依据被废止的指令的应被解释为依据本条例。凡是提及依据《数据保护指令》第 29 条设立的在个人数据处理中保护个人权利的工作小组的，应被解释为依据本条例设立的欧盟数据保护委员会。

第九十五条 本条例与《电子通信中的隐私保护指令》(Directive 2002/58/EC)的关系

鉴于《电子通信中的隐私保护指令》基于相同的目的规定了欧盟公共通信网络中公共电子通信服务中个人数据的处理方面的特别义务，本条例就此不应再对自然人或法人附加额外义务。

第九十六条 本条例与先前达成协议的关系

在 2016 年 5 月 24 日之前，成员国之间已达成的或者根据欧盟法律已制定的关于个人数据向第三国或国际组织转移的国际协议将继续有效，直至被修订、替代或撤销。

第九十七条 委员会报告

1. 至 2020 年 5 月 25 日前以及此后每四年，委员会应当向欧盟议会和理事会提交一份关于本条例的评估和审查报告。该报告应当公开。

2. 在第 1 款规定的评估和审查报告的前提下，委员会应当着重考察以下内容的实施运行：

（a） 第五章中个人数据向第三国或国际组织转移，特别是根据本条例第 45 条第 3 款做出的决定和根据《数据保护指令》第 25 条第 6 款做出的决定；

（b） 第七章中关于合作与一致性。

3. 为了实现第 1 款目的，委员会可以向成员国或监管机构要求提供信息。

4. 在执行第 1 款和第 2 款规定的评估和审查过程当中，委员会应当考虑到欧盟议会、理事会以及其他相关团体或信息提供者的立场和结论。

5. 如有必要，委员会应当提交适当的提案修订本条例，特别是考虑到信息技术的发展以及信息社会的进步。

第九十八条 其他欧盟数据保护法令的审查

在适当情况下，委员会为了确保处理过程中对自然人进行统一和一致保护， 应当提交立法提案修订关于个人数据保护的其他欧盟法令。尤其是欧盟机构、团体、部门、办事机构处理个人数据和数据的自由转移中的关于自然人保护的规定。

第九十九条 生效与实施

1. 本条例应在其于欧盟官方公报上发表之后的第二十日起生效。

2. 本条例自 2018 年 5 月 25 日起实施。

本条例在所有成员国范围内直接具有法律约束力。

（全文完）

更多金融科技资料与知识，请点击：www.dingxiang-inc.com。