译文丨欧盟 GDPR《一般数据保护法案》

编者按：2016 年 4 月 14 日，欧洲议会投票通过了商讨四年的《一般数据保护法案》（General Data Protection Regulation，GDPR），该法案将于 2018 年 5 月 25 日正式生效。GDPR 的通过意味着欧盟对个人信息保护及其监管达到了前所未有的高度，堪称史上最严格的数据保护法案。 GDPR 对于我国业务范围涉及欧盟成员国领土及其公民的企业进行合规运营、避免高昂处罚，以及对我国与数据相关的法学研究都具重要意义。

新法案由 11 章共 99 条组成，中文译本由中国政法大学互联网金融法律研究院（Internet financial law research institute of CUPL ,IFLRI）组织翻译。

第一章 一般规定

第 1 条 主题与目标

1. 本法就对与个人数据的处理相关的自然人的保护及个人数据的自由流动订立规则。

2. 本法保护自然人的基本权利和自由，尤其是自然人的个人数据保护权。

3. 不得以保护与处理的个人数据相关的自然人为由，限制或禁止个人数据在欧盟内部的自由流动。

第 2 条 适用范围

1. 本法适用于完全或部分以自动方式对个人数据的处理，构成或拟构成整理汇集系统一部分的自动方式除外。

2. 本法不适用于以下个人数据的处理：

(a) 发生在联盟法律范围之外的活动过程中;

(b) 由成员国在欧洲联盟条约第五卷第 2 章范围内进行活动时;

(c) 由自然人在纯粹的个人或家庭活动的过程中;

(d) 由主管当局为预防、调查、侦查或起诉的刑事犯罪，执行的刑事处罚的目的，包括防范和阻止公共安全受到威胁。

3. 欧盟机构、委员会、办事处和专业行政部门（代理机构）处理个人数据，适用第 45/2001 号条例。

根据本法第 98 条，处理个人数据适用第 45/2001 号条例和其他联盟法律法规的，应当符合本法的原则和规则。

4. 本法不影响 2000/31 / EC 指令的适用，特别是该指令第 12 条至第 15 条中的中间服务提供商的责任规则。

第 3 条 地域范围

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

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

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

(b) 是对数据主体发生在欧盟内的行为进行的监控的。

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

第 4 条 定义

为本法之目的：

(1) “个人数据”是指任何指向一个已识别或可识别的自然人（“数据主体”）的信息。该可识别的自然人能够被直接或间接地识别，尤其是通过参照诸如姓名、身份证号码、定位数据、在线身份识别这类标识，或者是通过参照针对该自然人一个或多个如物理、生理、遗传、心理、经济、文化或社会身份的要素。

（2）“处理”是指针对个人数据或个人数据集合的任何一个或一系列操作，诸如收集、记录、组织、建构、存储、自适应或修改、检索、咨询、使用、披露、传播或其他的利用，排列、组合、限制、删除或销毁，无论此操作是否采用自动化的手段。

（3）“处理限制”是指对已存储的个人数据的标识，用于在将来限制他们的处理行为；

（4）“剖析”是指为评估与自然人相关的某些个人情况，对个人数据进行任何自动化处理、利用的方式，特别是针对与自然人的工作表现、经济状况、健康状况、个人偏好、兴趣、信度、习性、位置或行踪相关的分析和预测。

（5）“匿名化”是一种使个人数据在不使用额外信息的情况下不指向特定数据主体对待个人数据处理方式。该处理方式将个人数据与其他额外信息分别存储，并且使个人数据因技术和组织手段而无法指向一个可识别和已识别的自然人。

（6）“整理汇集系统”是一种依照特定标准，如集中、分散或功能分布或地域基准存取个人数据的结构化集合。

（7）“控制者”是能单独或联合决定个人数据的处理目的和方式的自然人、法人、公共机构、行政机关或其他非法人组织。其中个人数据处理的目的和方式，以及控制者或控制者资格的具体标准由欧盟或其成员国的法律予以规定。

（8）“处理者”是指为控制者处理个人数据的自然人、法人、公共机构、行政机关或其他非法人组织。

（9）“接收者”是指接收到被传递的个人数据的，无论其是否是第三方的自然人、法人、公共机构、行政机关或其他非法人组织。但是，政府因在欧盟或其成员国法律框架内特定调查接收到个人数据的，不得被视为“接收者”；政府处理这些数据应当根据数据处理的目的，遵循可适用的数据保护规则。

（10）“第三方”是指数据主体、控制者、处理者以及在控制者或处理者直接授权处理个人数据者以外的自然人、法人、公共机构、行政机关或其他非法人组织。

（11）数据主体的“同意”是指数据主体依照其意愿自愿做出的任何指定的、具体的、知情的及明确的指示。通过声明或明确肯定的行为作出的这种指示，意味着其同意与他或她有关的个人数据被处理。

（12）“个人数据外泄”是指个人数据在传输、存储或进行其他处理时的安全问题引发的个人数据被意外或非法破坏、损失、变更、未经授权披露或访问。

（13）“基因数据”是指与自然人先天或后天的遗传性特征相关的个人数据。这类数据传达了与该自然人生理机能或健康状况相关的独特信息，并且上述数据往往来自于对该自然人生物样本的分析结果。

(14) “生物识别数据”是通过对自然人的物理、生物或行为特征进行特定的技术处理的得到的个人数据。这类数据生成了那个自然人的唯一标识，比如人脸图像或指纹识别数据。

（15）“有关健康的数据”是指与自然人身体或精神健康有关的个人数据，包括能揭示关于他或她的健康状况的健康保健服务所提供的数据。

（16）“主营业地”意味着：

(a)对于营业机构在多个成员国的的控制者，除非控制者在欧盟内的另一个营业机构能够决定并有能力贯彻个人数据的处理目的和方式，否则其在欧盟内的主要管理者所在地被视为主营业地。

(b) 对于营业机构在多个成员国的处理者，其在欧盟内的主要管理者所在地，在本法下承担特定义务；如果处理者在欧盟内没有主要管理者，在处理者的营业机构的营业范围内进行主要处理行为的营业地，在本法下承担特定义务。

(17) “代表”指由控制者和处理者依照第 27 条书面指定的，代表控制者和处理者分别履行本法规定的义务的欧盟内的自然人、法人。

(18) “企业”是指参与经济活动的自然人或法人，无论其为何种组织形式，可以包括合伙或经常性参与经济活动的协会。

(19) “企业团体”是指一个管控性的企业以及受其管控的企业群。

(20) “约束性企业规则”是指成员国领土上的控制者和处理者通过事业集团或企业集团进行的联合经济活动，而致个人数据传输或系列传输到一个或多个第三方国家的控制者或处理者时必须遵循的个人数据保护政策。

(21) “监管机构”是指一个独立的，由成员国依据第 51 条设立的公权力机构。

(22) “有关监管机构”是与人数据处理有关的监管机构，因为:

(a) 控制者或处理者是建立在监管机构所在的成员国领土上的；

(b) 居住在监管机构所在成员国的数据主体被或可能被处理行为严重影响；或

(c) 一个由监管机构提交的申诉；

(23)“跨境处理”是指以下情形之一：

(a) 个人数据处理发生在一个欧盟内的设立在多个成员国的控制者或处理者在多个成员国的营业机构的活动中。

(b) 个人数据的处理发生在一个欧盟内的控制者或处理者的唯一营业机构的活动中，但是这种处理严重影响或可能会严重影响多个成员国的数据主体。

(24) “相关与合理异议”是指一种关于是否存在违反本法情况，或是控制者或处理者是否存在遵守本法的预设行为的异议。这个异议清晰地表明了有关数

据主体的基本权利和自由的决议草案所造成的风险的重要影响，以及此种异议也适用于欧盟内的个人数据自由流动。

(25) “信息社会服务”是指欧洲议会和理事会的指令（欧盟）2015/1535 的第一条（1）款的（b）项中定义的服务。

(26) “国际组织”是指依照国际公法设立的组织及其下属机构，或依据或以两个或更多国家之间达成的协议为基础建立的其他机构。

第二章 原则

第 5 条 与个人数据处理相关的原则

1. 个人数据应：

(a) 以合法、公正、透明的方式处理与数据主体有关的（“合法性、公平性和透明性”）；

(b) 为特定的、明确的、合法的目的收集，并且不符合以上目的不得以一定的方式进行进一步的处理；为公共利益、科学，或历史研究目的，或统计目的而进一步处理，按照第 89 条第（1）款，不应被视为不符合初始目的（“目的限制”）；

(c) 充分、相关以及以该个人数据处理目的之必要为限度进行处理（“数据最小化”）；

(d) 准确，必要，及时；为了个人数据被毫不延迟地处理、删除或修正的目的，必须采取一切合理的步骤确保个人数据是不精确的（“精度”）；

(e) 在不超过个人数据处理目的之必要的情形下，允许以数据主体以可识别的形式保存；为了保护数据主体的权利和自由，依据第 89 条（1）予以实施本法所要求的适度的技术和组织措施，只要个人数据将仅仅以为达到公共利益、科学或历史研究或统计的目的而处理，个人数据能被长时间存储（“存储限制”）。

(f) 以确保个人数据适度安全的方式处理，包括使用适当的技术或组织措施来对抗未经授权、非法的处理、意外遗失、灭失或损毁的保护措施（“完整性和机密性”）。

2. 控制者应该负责，并能够证明符合第一项(“问责制”)。

第 6 条 处理的合法性

1. 只有在适用以下至少一条的情况下，处理视为合法：

（a）数据主体同意他或她的个人数据为一个或多个特定目而处理;

（b）处理是为履行数据主体参与的合同之必要，亦或处理是因数据主体在签订合同前的请求而采取的措施；

（c）处理是为履行控制者所服从的法律义务之必要；

（d）处理是为了保护数据主体或另一个自然人的切身利益之必要；

（e）处理是为了执行公共利益领域的任务或行使控制者既定的公务职权之必要；

（f）处理是控制者或者第三方为了追求合法利益的之必要，但此利益被要求保护个人数据的数据主体的利益或基本权利以及自由覆盖的除外，尤其是数据主体为儿童的情形下。

前第一款（f）项不适用于政府当局在履行其职责时进行的处理。

2.成员国可以维持或引入更具体的规定来适应本法关于处理的条款应用，通过设定包括在第九部分中规定的其他具体处理情形，设定更准确具体的处理要求和其他措施来确保合法和公平的处理，以遵守第一款的(c)项和(e)项，

3.第一款的(c)项和(e)项所指的处理的依据如下：

（a）欧盟法律；或

（b）控制者所属的成员国法律。

处理的目的应当依据法律确定，或者根据第一款（e）项中所指之处理，即应当为了执行公共利益领域的任务或行使控制者既定的公务职权之必要。法律依据可以包括具体条款以此来适应本法条款的应用，特别是：调整控制者处理合法性的一般条件；被处理的数据类型；与数据主体相关的；个人数据可能被披露的实体和目的；目的限制；存储期限；以及处理操作和处理程序，包括确保合法和公平处理的措施，诸如那些在第九部分提及的其他具体处理情况。欧盟或成员国法律应当符合公共利益的目标以及与追求的正当目标相称。

4. 当处理不是为了个人数据被收集时的那个目的，并且这个目的不是基于数据主体的同意，亦非基于在民主社会构成一个必要且适当措施来保障第 23 条（1）款所指之目标的欧盟或成员国法律，控制者应当为了查明为其他目的进行的处理是否与个人数据最初被收集时的目的相一致而考虑，特别是：

（a）任何在个人数据被收集时的目的和预期进一步处理的目的之间的联系；

（b）个人数据被收集时的情形，尤其是关于数据主体和控制者的关系的；

（c）个人数据的性质，尤其不管是依据第 9 条被处理的特殊类别的个人数据，还是依据第 10 条与刑事定罪和罪行有关的个人数据；

（d）预期进一步处理给数据主体可能造成的后果；

（e）适当的可能包括加密或匿名化的保障措施的存在。

第 7 条 同意的要件

1. 如处理是基于同意，则控制者应能证明数据主体已经同意处理他或她的个人数据。

2. 如数据主体通过书面声明的方式作出同意，且书面声明涉及其他事项，那么同意应以易于理解且与其他事项显著区别的形式呈现。构成违反本法的声明的任何部分，均不具约束力。

3. 数据主体有权随时撤回他或她的同意。同意的撤回不应影响在撤回前基于同意作出的合法的数据处理。在作出同意前，数据主体应被告知上述权利。撤回同意应与作出同意同样容易。

4. 当评估同意是否是自由作出时，应尽最大可能考虑，还应考虑合同的履行，包括服务的提供是否是基于对履行合同不必要的个人数据的同意。

第 8 条 关于信息社会服务适用于儿童同意的条件

1. 如适用第 6 条第 1 款（a）项，关于直接向儿童提供信息社会服务的，对 16 周岁以上儿童的个人数据的处理为合法。儿童未满 16 周岁时，处理只有在征得父母责任的主体同意情形下，或授权儿童同意的范围内合法。

如低龄不低于 13 周岁，则成员国可以通过法律为那些目的向低龄提供。

2. 考虑到现有技术，控制者应当作出合理的努力，去核实在此种情况下，父母责任的主体同意或授权。

3. 第 1 款不应影响成员国的一般合同法律，诸如与儿童有关的合同效力、构成或实行。

第 9 条 特殊种类的个人数据处理

1.对揭示种族或民族出身，政治观点、宗教或哲学信仰，工会成员的个人数据，以及以唯一识别自然人为目的的基因数据、生物特征数据，健康、自然人的性生活或性取向的数据的处理应当被禁止。

2.如果符合以下情形，则第 1 款不适用：

(a) 数据主体对以一个或数个特定目的对上述个人数据的处理给予了明确同意，但依照欧盟或者成员国的法律规定，第 1 款规定的禁止情形不能被数据主体援引的除外。

(b)数据处理为实现控制者或数据主体在工作、社会保障以及社会保障法的范畴内履行义务、行使权利之目的，则是必要。应当在欧盟或成员国的法律认可下，或者依据成员国对数据主体的基本权利和利益提供适当的保障的法律规定订立的集体协议的范围内实施。

(c) 数据处理是对于保护数据主体或另一个自然人的切身利益之必要，但数据主体物理上或法律上无法给予同意时；

(d) 数据处理是由政治、哲学、宗教、工会性质的协会、组织或其他非营利组织在有适当安全保障的合法活动中实施的，处理应当仅仅与该组织的成员或前成员或与该组织依组织宗旨为联系的定期联系人相关，并且相关个人数据未经数据主体同意不得向组织外的人披露。

(e) 处理被数据主体明显地公开的个人数据；

(f) 数据处理为合法诉求的成立、行使或辩护或者法庭司法权的行使之必要；

(g) 为了实质的公共利益，数据处理是必要的。依据欧盟或者成员国的法律，追求该目的是适当的，应当尊重数据保护的基本权利，应当提供适当、特定的措施来保障数据主体的基本权利和利益；

(h) 为实现以下目的，数据处理是必要的。为了预防医学和职业医学，为了雇员的工作能力评估，医疗诊断，提供卫生社会保健或治疗或卫生社会保健体系以及服务的构建，应当依据欧盟或成员国的法律或者依据与保健专业人士的合同，并且遵守第 3 款要求的条件和保障。

(i) 在公共健康的领域为了公共利益的考量，对于特定专业秘密的数据处理是必要的。譬如，抵御严重的跨境卫生威胁，确保卫生保健、药品或医疗器械高标准的质量和安全，依据联盟或成员国的法律规定以适当的、特定的措施来保障数据主体的权利与自由；

(j) 为了公共利益、科学或历史研究的目的，或者统计的目的，依照第 89 条第（1）款基于联盟或者成员国的法律，追求该目的是适当的，应当尊重数据保护的基本权利，应当提供适当、特定的措施来保障数据主体的基本权利和利益。

3.为实现第 2 款（h）项中的目的，第 1 款中的个人数据可能被处理，那些数据应当被一个依据欧盟或者成员国的法律或国家法定机构制定的规则负有保守专业秘密的义务的专业人士处理，或者说这是他的责任；或者由另一个同样依据欧盟或者成员国的法律或国家法定机构制定的规则遵守保密义务的人处理。

4. 成员国可以保持或者引进进一步的条件，包括指向基因数据、生物特征数据或者健康数据的个人数据处理的限制。

第 10 条 有关刑事定罪和罪行的个人数据的处理

有关刑事定罪和罪行的，或有关基于第 6 条第 1 款的安全措施的个人数据的处理应当在公务职权的控制下开展，或者被欧盟或成员国法律授权为保护数据主体的自由和权利而提供保护措施的处理。任何刑事定罪的综合登记应当只能在公务职权的控制下保存。

第 11 条 无需认证的处理

1.如果控制者不需要或者不再需要认证其所掌控的个人数据的数据主体，那么若仅仅根据本章程的要求和规定，控制者就没有义务保存、获取或者处理额外的信息来认证数据主体。

2.如果有本条第一款所提到的情况，那么在可能的情况下，控制者应当告知数据主体，说明自己并无对数据主体进行认证的职责。只有在数据主体出于行使自身权利需要，而且提供额外的身份证明信息的情况下，第 15 条至第 20 条才能得以适用。

第三章 数据主体权利

第一节 信息透明度和信息机制

第 12 条 数据主体行使权利的透明度、交流和模式

1.控制者应当以一种简单透明、明晰且容易获取的方式，通过清楚明确的语言，采取合适措施提供第 13 条和第 14 条所提到的任何信息，以及根据第 15 条到第 22 条和第 34 条所提及的关于数据主体处理过程的沟通信息（尤其是关于儿童的任何信息）。控制者应当提供书面材料，在其他情况下，若有必要，可以采用电子方式。如果数据主体能够通过其他方式得到认证，那么在数据主体的要求下，能够以口头方式提供信息。

2.控制者应当根据第 15 条到第 22 条的规定帮助数据主体行使权利。在第 11 条第 2 款的情形下，除非控制者说明自己不具有数据主体的认证职责，否

则，对于数据主体根据第 15 条至第 22 条行使自身权利的要求，控制者不能拒绝。

3.控制者应当及时（在任何情况下不得超过一个月）提供根据第 15 条至第 22 条采取的行动信息。考虑到要求的复杂性和数量，在必要的时候，这一期限可以再延长两个月。对于延期提供信息的任何情况，控制者都应当通知数据主体相关情形和延迟原因。在可能的情况下，这些信息能够以电子方式提供，除非数据主体对提供方式有特殊要求。

4.如果控制者没有根据数据主体的要求采取行动，控制者应当及时通知（至迟不超过一个月）数据主体未采取行动的原因、向监督机构提起申诉以求寻求司法救济的可能性。

5.根据第 13 条和第 14 条所提供的信息以及根据第 15 条至第 22 条和第 34 条提供的任何沟通行动都应当免费提供。在数据主体提出的要求无法查明、超出提供范围，尤其是重复提起要求的情形下，控制者也可以：

（a）考虑到提供信息、交流或者采取行动的行政成本，行政部门可以收取合理的费用；

（b）拒绝受理数据主体的请求。

控制者应当承担说明那些无法查明或者居于其提供范围之外的数据的责任。

6.在不违背第 11 条的前提下，控制者在对自然人依据第 15 条到第 22 条所提出的要求持有合理怀疑时，可以要求数据主体提供额外的必要的信息来证明身份。

7.根据第 13 条和第 14 条的要求，控制者应当采用标准化的图标，以简洁明了、清晰可视、晓畅易读的方式向数据主体提供信息。这些图标以电子方式呈现，这样就可以以机读的方式进行信息的读取工作。

8.欧盟委员会应当被授予根据第 92 条的规定采取措施来制定标准化图标的信息和程序的权利。

第 2 节 个人数据信息和获取

第 13 条 数据主体收集的个人数据的提供

1.鉴于数据主体能够获取与自身有关的个人数据，控制者应当在获取个人信息时，向数据主体提供以下信息：

（a）控制者的身份和详细联系方式，适当时还要提供代表人的身份和详细联系方式；

（b）适当时提供数据保护局的详细联系方式；

（c）个人信息处理的目的以及处理的法律基础；

（d）当处理过程是依据（f）项和第 6 条第一款的规定进行的，应当说明控制者或者第三方追求的立法利益；

（e）如果可以，应当提供个人数据接收方或者接受方的种类；

（f）在适当的情况下，应当提供控制者意图将个人数据向第三国或者国家组织进行传输的事实、委员会是否就此问题做出过充分决议、第 46、47 条或者第 49 条第 1 款第二小段提及情形的相关信息。此外，还包括所采取的保护个人信息的合理安全措施以及获取复印件的方式。

2.除了第一款提到的信息，控制者在获取个人数据时，出于证实处理过程的公正和透明的需要，在必要的情况下，应当向数据主体提供如下信息：

（a）个人数据的储存阶段，在无法提供的情形下，应当提供阶段划分的决定标准；

（b）有资格处理数据主体权利要求的，能够获取、修正、删除个人信息或者管制数据权利的控制者的信息；

（c）根据第 6 条（a）项或者第 9 条第 2 款（a）项所进行的在不触犯法律的前提下，处理过程信息、任意取消满意度的相关信息；

（d）向监督机构提起申诉的权利；

（e）个人数据条款是否应当在法律条文中、在合同契约中规定。还是应当作为缔结合同的必要条件进行规定。此外，还应当包括数据主体是否有义务提供个人数据以及无法提供数据情形下的可能的后果的信息；

（f）自动的决策机制，包括第 22 条第 1 款以及第 4 款提到的分析过程所涉及的逻辑程序以及对数据主体的处理过程的重要意义和设想结果。

3.鉴于控制者进一步处理个人信息的意图，控制者应当在此之前向数据主体提供与第 2 款有关的信息。

4.当数据主体已经获得这些信息时，第 1 款、第 2 款、第 3 款不能得以适用。

第 14 条 并非从数据主体处获取的个人数据的提供

1.当个人信息并非从数据主体处获得时，控制者应当向数据主体提供如下信息；

（a）控制者的身份和详细联系方式，适当时还要提供代表人；

（b）适当时提供数据保护局的详细联系方式；

（c）个人信息处理的目的以及处理的法律基础；

（d）相关个人数据的种类；

（e）个人数据接收方或者接受方的种类；

（f）在适当的情况下，应当提供控制者意图将个人数据向第三国或者国家组织进行传输的事实、委员会是否就此问题做出过充分决议、第 46、47 条或者第 49 条第 1 款第二项提及情形的相关信息。此外，还包括所采取的保护个人信息的合理安全措施以及获取复印件的方式。

2.除了第一款提到的信息，控制者在获取个人数据时，出于证实处理过程的公正和透明的需要，在必要的情况下，应当向数据主体提供如下信息：

（a）个人数据的储存阶段，在无法提供的情形下，应当提供阶段划分的决定标准；

（b）鉴于第 6 条第 1 款（f）项的处理过程，控制者或者第三方追求的立法利益；

（c）有资格处理数据主体权利要求的，能够获取、修正、删除个人信息或者管制数据权利的控制者的信息；

（d）根据第 6 条第 1 款（a）项或者第 9 条第 2 款（a）项所进行的在不触犯法律的前提下，处理过程信息、任意取消满意度的相关信息；

（e）向监督机构提起申诉的权利；

（f）个人数据获取的来源，在合适的情况下，提供是否是通过公共方式获取的信息；

（g）自动的决策机制，包括第 22 条第 1 款以及第 4 款提到的分析过程所涉及的逻辑程序以及对数据主体的处理过程的重要意义和设想结果。

3.控制者应当根据第 1 款和第 2 款的规定提供信息：

（a）在获取个人数据之后的合理期限内（至迟不超过一个月），提供与个人数据获取具体情形有关的信息；

（b）如果个人数据将要用于数据主体间的交流，那么信息提供时间最迟不超过第一次交流活动；

（c）如果可以披露接收方，那么信息提供时间最迟不晚于个人数据的首次披露时间。

4.鉴于控制者进一步处理个人信息的意图，控制者应当在此之前向数据主体提供与第 2 款有关的信息。

5.第 1 款至第 4 款在以下情形不得适用：

（a）数据主体已经获得这些信息；

（b）这些信息的提供是不可能的，尤其是根据第 89 条第 1 款规定或者本条第 1 款提及的义务规定，出于公共利益、科学或者历史调查和统计调查的目的所进行的不均衡的努力。在这些情况下，控制者应当采取合适的措施去保护数据主体的权利和自由以及法律利益（包括公开信息的措施）；

（c）控制者应当根据联盟或者成员国法律所规定的获取或者披露个人信息的规定，采取合适的措施来保护数据主体的法律利益；

（d）根据联盟或者成员国法律以及保密法规定的职业保密制度，个人数据必须保密。

第 15 条 数据访问权

数据主体应当有权从管理者处确认关于该主体的个人数据是否正在被处理，以及有权在该种情况下访问个人数据和以下信息：

（a）处理的目的；

（b）有关个人数据的类别；

（c）个人数据已经被泄露或者将会被泄露给的接受者或接受者类别，特别是第三国或国际组织的接受者；

（d）在可能的情况下，预想的个人数据存储期间；或者不可能时，用于确定该期间的标准；

（e）有权要求管理者纠正或删除该个人数据或者限制或拒绝处理关于该数据主体的个人数据；

（f）向监管机构提出投诉的权利；

（g）在个人数据并非由数据主体收集的情况下，关于其来源的任何可用信息。

（h）自动化决策，包括第 22 条第 1 款和第 4 款提到的概要，以及涉及到的至少在前述情况下有意义的逻辑方面的信息，和这种处理行为对数据主体而言的意义和预想的后果。

如果将个人数据转移到第三国或国际组织，数据主体应当有权根据第 46 条获得有关转让的适当保障的通知。

控制者应提供正在处理的个人数据的副本。对于数据主体要求的任何进一步的文本，控制者可以根据管理成本收取合理的费用。如果数据主体通过电子方式提出请求，除非数据主体另有要求，信息应当以常用的电子形式提供。

获得第 3 款所指副本的权利不得对他人的权利和自由产生不利影响。

第 16 条 纠正权

数据主体应当有权要求控制者无不当延误地纠正有关其的不准确个人数据。考虑到处理的目的，数据主体应当有权使不完整的个人数据完整，包括通过提供补充声明的方式。

第 17 条 擦除权（被遗忘权）

数据主体有权要求控制者无不当延误地删除有关其的个人数据，并且在下列理由之一的情况下，控制者有义务无不当延误地删除个人数据：

（a）就收集或以其他方式处理个人数据的目的而言，该个人数据已经是不必要的；

（b）数据主体根据第 6 条第 1 款（a）项或第 9 条第 2 款（a）项撤回同意，并且在没有其他有关（数据）处理的法律依据的情况下；

（c）数据主体根据第 21 条第 1 款反对处理，并且没有有关（数据）处理的首要合法依据，或者数据主体根据第 21 条第 2 款反对处理；

（d）个人数据被非法处理；

（e）为遵守控制者所受制的联盟或成员国法律规定的法定义务，个人数据必须被删除；

（f）个人数据是根据第 8 条第 1 款所提及的信息社会服务的提供而收集的。

如果控制者已将个人数据公开，并且根据第 1 款有义务删除这些个人数据，控制者在考虑现有技术及实施成本后，应当采取合理步骤，包括技术措施，通知正在处理个人数据的控制者，数据主体已经要求这些控制者删除该个人数据的任何链接、副本或复制件。

当处理（数据）对于以下情形而言是必要的时，第 1 款和第 2 款不应当被适用：

（a）为了行使言论和信息自由的权利；

（b）为了遵守需要由控制者所受制的联盟或成员国法律处理的法定义务，或为了公共利益或在行使被授予控制者的官方权限时执行任务；

（c）根据第 9 条第 2 款（h）、（i）项以及第 9 条第 3 款，为了公共卫生领域的公共利益的原因；

（d）根据第 89 条第 1 款，为了公共利益的存档目的、科学或历史研究目的或统计目的，只要第 1 款所述的权利很可能表现为不可能的或者很可能严重损害该处理目标的实现；

（e）为了设立、行使或捍卫合法权利。

第 18 条 限制处理权

在下列情况之一，数据主体应当有权限制控制者处理（数据）：

（a）数据主体对个人数据的准确性提出争议，且允许控制者在一定期间内核实个人数据的准确性；

（b）该处理是非法的，并且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；

（c）控制者基于该处理目的不再需要该个人数据，但数据主体为设立、行使或捍卫合法权利而需要该个人数据；

（d）数据主体在核实控制者的法律依据是否优先于数据主体的法律依据之前已根据第 21 条第 1 款反对处理。

如果处理（行为）根据第 1 款受到限制，除储存之外，这些个人数据只应在数据主体同意的情况下，或为设立、行使或捍卫合法权利，或为保护其他自然人或法人的权利，或为了联盟或成员国的重要公共利益的原因被处理。

根据第 1 款有权限制处理（数据）的数据主体应当在处理限制解除之前收到控制者的通知。

第 19 条 关于纠正或删除个人数据或限制处理的通知义务

除非被证明不可能完成或者包含不成比例的工作量，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，传达给已向其披露个人数据的接收者。

如果数据主体请求，控制者应当通知数据主体这些接收者。

第 20 条 反对权

数据主体有权基于与其特定情况有关的理由，在任何时候依据第 6 条第 1 款（e）项或（f）项拒绝有关其的个人数据被处理，包括根据这些规定进行概况分析。控制者不得再处理该个人数据，除非控制者证明其有关（数据）处理的强制性法律依据优先于数据主体的利益、权利和自由，或者为了设立、行使或捍卫其合法权利。

如果为了直接营销的目的而处理个人数据，数据主体有权在任何时候反对有关其的个人数据为进行此类营销而被处理，其中包括与此类直接营销相关的概况分析。

如果数据主体反对以直接营销为目的的处理，则个人数据不得再为此目的而被处理。

最迟在与数据主体第一次通信时，第 1 款和第 2 款中提到的权利应当明确提请数据主体注意，并应清楚地、与任何其他信息分开提交。

第四节 拒绝权和自主决定权

第 21 条 拒绝权

1. 数据主体拥有拒绝权，在关于他/她的特定情形下，在任何时间处理关系到他/她第 6 条第 1 款第（e）或第（f）项规定的个人数据，包括基于这些条款的分析。控制者不能处理个人数据，除非控制者能够证明不顾数据主体的利益、权利和自由处理数据或者建立、行使或维护这种法律权利具有令人信服的正当化理由。

2. 个人数据因为直接营销的目的被处理的，数据主体应当有权利拒绝在任何时间因为这种商业目处理关系到他/她的个人数据，这种商业目的包括分析达到有关这种直接营销的程度。

3. 数据主体拒绝因直接的商业目的处理数据的，个人数据不应该因任何这种目的被处理。

4. 至少在与数据主体第一次沟通时，在第一款和第二款指代的权利应该明确地提起数据主体的注意，应该被清晰地呈现且与任何其他的信息相区分。

5. 在信息社会服务使用的背景下，即使有欧共体 2002 年的指令，数据主体可以通过使用技术规范的自动化方式行使他/她的拒绝权。

6. 根据第 89 条第 1 款个人数据因科学或历史研究或统计的目的被处理的，数据主体在关于他/她的特定情形下，有权利拒绝对他/她的个人数据进行处理，除非这种处理对于一个因为公共利益的任务的履行是必要的。

第 22 条 自主化的个人决策，包括分析

1. 数据主体有权利不受一个仅仅依靠包括分析的自动化处理的决定的限制，这会产生关于他/她或仅仅影响他/她的法律后果。

2. 第一款不适用，如果这个决定：

（a）对于数据主体和一个数据控制者之间的一个合同的建立和履行是必要的。

（b）这个控制者是数据主体，以及确立保护数据主体权利、自由和正当化利益的适当措施是联盟或成员国的法律所规定的；或

（c）基于数据主体的明确同意。

3. 在涉及到第 2 款第（a）和（c）项的情况下，数据控制者应当实施适当的措施保护数据主体的权利、自由和正当化利益，至少获得对控制者部分的人为干预权，表达他/她的观点和争夺决定权。

4. 在第二款涉及的决定不应当基于第 9 条第 1 款提及的个人数据的特殊分类，除非适用第 9 条第 2 款的第（a）或（g）项和确立适当的措施维护数据主体的权利、自由和正当化利益。

第五节 限制

第 23 条 限制

1. 联盟或成员国的法律规定数据控制者或处理者是主体，可以通过立法措施限制第 12 条至 22 条和第 34 条的权利与义务的范围，以及第 5 条中与在第 12 条至 22 条的权利义务相对应的条款。这样一种限制尊重了基本权利和自由的本质，是一种在民主社会必要的、相符合的措施，以此维护：

（a）国家安全；

（b）防卫；

（c）公共安全；

（d）刑事犯罪的预防、调查、侦查、起诉或者刑事处罚的执行，包括对公共安全威胁的防范和预防；

（e）联盟或一个成员国一般公共利益的其他重要目标，特别是联盟或成员国的重要经济或财政利益，包括货币、预算和税收等事项、公共卫生和社会保障；

（f）司法独立与司法程序的保护；

（g）违反职业道德规范的预防、调查、侦查和起诉；

（h）监督、检查或相关的监管职能，甚至偶尔行使官方权力在涉及到第（a）（b）（c）（d）（e）（f）和（g）项的情形下。

（i）对数据主体或其他人的权利与自由的保护。

（j）民事诉讼赔偿的执行。

2. 特别是，在第 1 款所指的任何立法措施，应至少包含具体的规定，有关的，如：

（a）处理的目的或处理的分类；

（b）个人数据的分类；

（c）引入的限制范围；

（d）防止滥用或非法使用或转让的保障措施；

（e）控制者的具体说明或控制者分类；

（f）存储期限和适用的保障措施，考虑到性质、范围和处理的用途或处理的分类；

（g）对数据主体权利和自由的威胁；和

（h）数据主体被告知限制的权利，否则将不利于限制的目的。

第四章 控制者和处理者

第一节 基本义务

第 24 条 控制者的义务

1. 考虑到性质、范围、内容和处理的用途以及处理给自然人的权利和自由带来的不同可能性和严重程度的风险，控制者应当实施适当的技术和组织措施，以确保并能够证明，根据本条例进行处理。这些措施应在必要时进行审查和更新。

2. 有关处理活动相称的，第 1 款所指的措施应包括由控制者实施适当的数据保护政策。

3. 遵守第 40 条提及的行为准则或第 42 条提及的经批准的认证机制，可以作为一个元素，以证明符合控制者的义务。

第 25 条 通过设计和默认的数据保护

1. 考虑到现状，执行的成本和性质，范围，内容和处理的用途以及处理给自然人的权利和自由带来的不同可能性和严重程度的风险，控制者应该在确定处理手段和在处理的同时，实施适当的技术和组织措施，如匿名化，即目的是实施数据保护原则，如数据最小化，以有效的方式，在处理时实施必要的保障措施，以符合法律要求，保护数据主体的权利。

2. 控制者应该实施适当的技术和组织措施以确保，在默认情况下只有对每个特定处理目的有必要的个人数据才能被处理。该义务适用于收集的个人数据的数量，数据处理的程度，数据的存储期限和数据的可及性。特别是，这些措施应确保在没有个人对无限数量自然人的干预下，个人数据在默认情况是不可访问的。

3. 根据第 42 条的经批准的认证机制可以作为一个元素，以证明符合本条第 1 款和第 2 款的要求。

第 26 条 联合控制者

1. 当由两个或两个以上的控制者共同决定处理的目的和手段时，他们就是联合控制者。他们应以明确的方式确定在监管规定下各自的责任与义务，尤其是通过他们之间的安排，确定关于行使数据主体的权利和第 13 条和 14 条提及的他们各自的提供信息的职责，除非到目前为止，控制者各自的责任由联盟或成员国法律确定哪些控制者是主体。这种安排可以指定数据主体的联系点。

2. 第一款提到的安排应当及时反映各自的角色和联合控制者相对数据主体的关系。该安排的实质，应使数据主体得知。

3. 不论在第 1 款所指的安排条款，数据主体可以根据本规定行使他或她的权利，不论是否与控制者一致。

第 27 条 未在联盟中设立的控制者或处理者的代理人

1. 如果适用第 3 条第 2 款的，控制者或处理者应当以书面形式指定联盟中的代理人。

2. 该义务不适用于：

（a）偶然的处理，在一个大的范围里，不包括对第 9 条第 1 款提及的数据的特殊类别的处理，或者第 10 条提及的有关刑事定罪和处罚的个人数据的处理，而且考虑到处理的性质、内容、范围和目的，这种处理不太可能导致自然人的权利和自由的风险；或者

（b）一个公共权力机关或机构。

3. 代理人应当被建立在一个成员国中，这些成员国的数据主体及其个人数据根据提供给它们的货物或服务被处理，或者它们的行为被监控。

4. 为确保遵守本条例的目的，代理人应被控制者或处理者授权，以及特别是监管机构和数据主体的授权来处理所有的相关问题。

5. 控制者或处理者对代理人的指定，应对于代理人可能做出的不利于控制者或处理者自身的法律行为无损权益。

第 28 条 处理者

1. 当处理是以控制者的名义进行的，控制者只使用处理者实施的适当的技术和组织措施提供充分保证，以这种方式使处理满足法规的要求，确保对数据主体权利的保护。

2．如果未经控制者特别的或一般的的事先书面授权，该控制者不能引入另一个控制者参与。在一般的书面授权的情况下，处理者应该通知控制者任何有关增加或替换其他控制者的变化，以使控制者有机会应对这样的变化。

3. 一个处理者的处理应遵守联盟或成员国法律下的在合同或其他法律行为，即控制者与处理者相结合，提出处理的主题和处理的期限，性质和处理目的，个人数据的类别、数据主体的分类和控制者的权利义务。该合同或其他法律行为应规定，特别是处理者：

（a）处理个人数据只能基于控制者的书面指示，包括有关个人数据向一个第三世界国家或一个国际组织的转移，除非联盟或成员国法律所允许这样做

的，该处理者是主体；在这种情况下，处理者在处理之前，应通知控制者有关法律的要求，除非法律由于重大公共利益的原因禁止提供这样的信息；

（b） 确保个人被授权处理个人数据，且已承诺保密或在适当的法定保密义务下；

（c）根据第 32 条要求的采取所有措施；

（d）遵守第 2 款和第 4 款提到的引入其他处理者的条件；

（e）考虑到处理的性质，运用适当的技术和组织措施协助控制者，因为到目前为止这是可能的，为履行控制者的义务，以适应第三章规定的行使数据主体权利的要求；

（f）考虑到处理的性质和处理者可得到的信息，协助控制者以确保其遵守第 32 条至 36 条规定的义务；

（g）一旦选择了控制者，就需要删除或向该控制者返还所有的个人数据，在提供有关处理服务的最后，删除现有的版本，联盟或成员国法律允许存储的个人数据除外；

（h）提供给控制者所有必要的信息，以证明符合在本条中规定的义务，并允许和促进审计，包括检查，由控制者或由控制者授权的另一核数师进行。

关于第一项的第 h 项，处理者应当立即通知控制者，如果在其看来，一个指令违反了本条例或其他联盟或成员国的数据保护规定。

4. 在处理者引入其他处理者执行代表控制者的特定处理活动，第 3 款提及的控制者和处理者之间的合同或其他法律行为中的相同的数据保护的要求，应通过联盟或成员国法律在合同或其他法律行为施加给其他处理者，特别是实施适当的技术和组织措施提供充分保证，以这样的方式，确保处理能满足本规范要求。其他处理者未能履行其数据保护义务的，最初处理者应保持就其他处理者义务的履行对控制者承担责任。

5. 第 40 条所提及的一个处理者遵守的一个被认可的行为准则，或在第 42 条提及的一个经批准的认证机制，可以作为一个元素用来证明本条的第 1 款和第 4 款中提到的充分保证。

6. 在不损害控制者和处理者之间的单个合同情况下，在本条第 3 款和第 4 款提及的合同或其他法律行为，可能基于，本条第 7 款和第 8 款提及的标准化的合同条款的全部或部分，包括当它们成为依据第 42 条和第 43 条授权给控制者和处理者的认证的一部分。

7. 欧盟委员会可就本条第 3 款和第 4 款所指的事项制定标准化的合同条款，并按照第 93 条第 2 款所指的审查程序。

8. 监督机关可以采用根据本条第 3 款和第 4 款所指事项的标准化的合同条款，并按照第 63 条所指的一致性机制。

9. 第 3 款和第 4 款所指的合同或其他法律行为，应当以书面形式，包括电子形式；

10. 在不损害第 82 条、83 条和 84 条的情况下，如果一个处理者违反本条例的规定决定处理的目的和手段，该处理者可以在处理方面被认为是控制者。

第 29 条 在控制者或处理者的权限下处理

有权访问个人数据的处理者以及在控制者或处理者的权限下作为的任何人，除控制者指令外不得处理那些数据，除非联盟或成员国法律允许这么做。

第 30 条 处理活动的记录

1. 每一位控制者，以及如适用控制者的代理人，应当依其职责保持处理活动的记录。那个记录应当包括以下所有信息：

（a）控制者以及如适用的联合控制者、控制者代理人和数据保护员的姓名和联系信息；

（b）处理的目的；

（c）数据主体的类别和个人数据的分类的描述；

（d）个人数据已经或将要被公开的收件人的类别，包括在第三世界国家或国际组织的收件人；

（e）如适用，将个人数据向第三世界国家或国际组织的传输，包括该第三国或国际组织的鉴定，以及在第 49 条第 1 款第二款提及的传输的情况下，对文档采取适当的安全措施；

（f）如可能，则对擦除不同类别的数据设定时间限制；

（g）如可能，对第 32 条第 1 项提及的技术和组织安全措施进行一般性描述。

第 31 条 和监督机构的合作

在事务执行的过程之中，应用控制者、应用处理者以及它们的代表，应当根据要求与监管机构进行合作。

第 32 条 处理过程的安全性

1.统筹考虑最先进的技术、实施成本、处理过程（包括其性质、范围、目的）以及自然人自由权利变化可能性和严重性的风险。控制者、处理者应当执行合适的技术措施和有组织性的措施来保证合理应对风险的安全水平，尤其要酌定考虑以下因素：

（a）个人数据的匿名化和加密；

（b）数据系统保持持续的保密性、完整性、可用性以及弹性的能力；

（c）在发生自然事故或者技术事故发的情况下，存储有用信息以及及时获取个人信息的能力；

（d）定期对测试、访问、评估技术性措施以及组织性措施的有效性进行处理，力求确保处理过程的安全性。

2.安全账户的等级评估应当尤其重视处理过程中的风险问题，特别是抵御意外和非法销毁、损失、变更、未经授权披露或者是个人数据的传送、存储和处理过程中的风险。

3.参考第 40 条采取一种合法行为或者参考 42 条采取一种认证机制，这可以用来说明本条第一款要求的合规性。

4.控制者以及处理者应当逐步采取措施，以求确保在部门规制之下操作个人数据的自然人不能对数据进行处理，除非获得控制者的指示，或者其根据联邦或州宪法确有必要。

第 33 条 监管机构对个人数据泄露的通知

1.在个人数据泄露的情况下，控制者不能不当延误，而且至少应当在知道之时起 72 小时以内，根据第 55 条向监管机构进行通知，除非个人数据的泄露不会导致自然人权利和自由的风险。如果通知迟于 72 小时，需要对迟延原因进行解释。

2.在控制者知道发生信息泄露而不当延误时，处理者应当通知控制者。

3.第一款所说的通知，至少应当包括：

（a）对于所泄露的个人数据的性质进行描述，包括相关数据主体以及数据记录的种类和大致数量；

（b）和数据保护局或者是其他获取更多信息的联系点交流名称和联系方式；

（c）描述个人信息泄露的可能情况；

（d）重视个人数据泄露问题，描述控制者采取的或者计划采取的措施，包括在适当情况下能够减轻可能的负面影响的措施。

4.只要没有造成不适当的进一步延误，在信息不可能同时提供的情况下可以分阶段进行。

5.控制者应当记录任何个人数据泄露情况，包括和个人数据泄露有关的事实、影响和采取的补救性措施，这些可以使得监管机构验证行为的合规性。

第 34 条 关于数据主体的个人数据交流

当个人数据泄露可能对自然人权利和自由形成很高的风险时，控制者应当毫不延误地就个人数据泄露的主体进行交流。

本条第一款提到的数据主体交流，应当至少应当包括第 33 条第三款的（b）（c）（d）三项所涉及的信息和建议，并且用清晰平实的语言描述个人数据泄露的性质以及内容。

在一下这些情况下，不能适用第一款所提到的数据主体交流：

（a）控制者已经采取合适的技术性、组织性保护措施，而且此类措施已经被应用于受到信息泄露影响的个人信息之中，尤其是那些未经授权任何人都无法得知的技术，比如，数据加密技术；

（b）控制者已经采取能够确保第一款所提到的（自然人）权利和自由不受侵犯的高风险不再可能实现的措施。

（c）这会涉及到不相称的努力。在这样的情况下，就应当有一个能够使得数据主体获得平等有效通知的公共交流机制或者相类似的举措。

如果控制者并未就数据主体进行个人数据交流，考虑到个人数据信息泄露的高度风险，监管机构可以要求其这样做或者可以决定其符合第三款列出的任何条件。

第三节 数据保护影响评估以及事先咨询

第 35 条 数据保护影响评估

1.鉴于一种数据处理方式，尤其是使用新技术进行数据处理，统筹考虑处理过程的性质、范围、内容和目的，（不难得知）这很可能对自然人权利和自由带来高度风险。在进行数据处理之前，控制者应当对就个人数据保护所设想的处理操作方式的影响进行评估。一个单一的评估方法也许能够对目前的相似的高风险状况，提供相类似的一组操作方式。

2.当进行数据保护影响评估时，受委任的控制者可以向数据保护局寻求帮助。

3.以下情形尤其适用于第一款所说的数据保护：

（a）对自然人个人情况评估所进行的系统和广义上的理解也是基于自动处理（包括分析）以及基于依据

（b）第 9 条第一款提到的大范围的数据处理或者第十条提到的关于刑事定罪和罪行相关的个人信息。

（c）一个大规模的公共可访问区域的系统性监测。

4.监督机构应当根据第一款，建立并且公布一套数据处理机制，使其符合评估影响的需要。监管机构应当就这些与第 68 条所提到的董事会进行交流。

5.监督机构也可以建立以及向公众发布并不强制要求数据评估保护的处理机制种类。监管机构应当就此与董事会进行交流。

6.在采取第四款第五款的措施之前，监管机构应当应用 63 条的监管机制，包括与货物提供、服务提供、数据主体或者某些成员国的行为管控相关或者与可能会实质上影响到个人数据自由运动相关的处理活动。

7.评估至少包括以下内容：

（a）对于所设想机制以及处理目的（包括数据应用、控制者追求的立法利益）的系统性描述；

（b）对与处理目的相关的处理机制必要性的评估；

（c）对第一款所提到的数据主体的权利自由的风险性评估；

（d）所设想的处理风险的举措，包括保障措施、安全措施、确保个人数据保护安全的机制以及说明数据主体权利和立法利益方面的合规性举措。

8.在评估处理机制影响的过程中，对于 40 条所规定的相关管理者以及处理者行为的合法性应当考虑在内，尤其是关于数据保护评估目的的部分。

9.合适的情况下，管理者应当寻求数据主体或者他们在预期处理方面的代表的观点，不能对商业利益保护、个人利益保护或者处理机制的安全保护持有偏见。

10.依据第六条第一款（c）项或（e）项的处理，有联盟法律或者成员国国内法的依据，在这些法律之中，管理者是一方主体。这些法律规制了具体的处理方式或者一系列仍受争议的的机制。数据保护影响评估方式已经被当做是一般影响评估的一个部分得到实施。第一款到第七款不能得到适用，除非成员国认为处理活动的事先评估确有必要。

11.必要时，如果处理方式是根据数据保护影响评估所作出的，在处理机制的风险出现变化的时候，处理管理者应当对评估进行审查。

第 36 条 事先咨询

1.第 35 条下的数据保护影响评估表明，如果控制者没有采取措施减少风险，那么处理过程将会是高风险的。因而，控制者应当在处理之前向监督机构进行咨询。

2.第一款中监管机构预期处理在控制者没有完全认定或者减少风险的情况，是对第一款规定的违反。监督机构应当至迟在 8 周以内向控制者提出书面建议，也可以使用第 58 条所规定的权力。考虑到预期处理的复杂性，这一期限可以延迟六周。监管机构应当就任何延长期间的情况通知控制者以及处理者，并且说明迟延理由。这些期间可以中止，直到监管机构实现它所要求的咨询目的。

3.根据第一款向监管机构咨询时候，管理者应当提供：

（a）控制者，控制者和处理者的联合部门的代表职责，尤其是关于处理过程的企业团体；

（b）预期处理的目的和手段；

（c）根据本法保护数据主体权利自由的保障措施；

（d）应用时，数据保护局的联系方式；

（e）35 条所规定的数据保护影响评估；

（d）其他。

4.成员国应当在准备方案期间向监管机构咨询国家议会所指定的立法措施，或者基于这些立法措施且和数据处理有关的规章。

5.根据第一款，成员国的法律也许需要先向控制者咨询，对于涉及公共利益（包括社会保护和公众健康）的处理程序，应当获得监管机构的预先授权。

第四节 数据保护局

第 37 条 数据保护局人员的指派

1.在以下情况下，控制者和处理者应当指派数据保护人员：

（a）公共当局或者机构施行的处理措施，而非法院基于行使司法权进行的；

（b）控制者或者处理者数据处理机制的核心活动是性质、范围和（或者）目的，需要进行定期和系统的大规模数据主体监控；

（c）根据第 9 条的大规模特殊种类数据处理方式 以及第 10 条的刑事指控和犯罪，控制者和处理者的核心活动构成大规模的特殊数据种类；

2.如果可以在企业指派数据保护人员，企业团体可以任命一个独立的数据保护人员。

3.鉴于控制者和肩负按部门是一种公共的部门或者机构，考虑到它们的组织结构和规模，独立的数据保护人员可以被一些这样的部门或者机构所指派。

4.除了第一款所涉及的情况，控制者、处理者、处理协会、其他代表不同种类的部门或者根据联盟或者成员国法律应当设立的部门，应当指派数据保护人员。数据保护人员可以根据这些机构以及代表控制不嗯或者处理者的其他主题进行活动。

5.数据保护人员的指派应当给予职业能力，尤其是关于数据保护法律的专业知识以及 39 条所提到的完成任务的经验和能力。

6.数据保护人员可以是控制者或者处理者的成员，他们基于一种服务上的联系完成任务。

7.控制者或者处理者应当公布数据保护人员的联系方式，并且将名旦告知监管机构。

第 38 条 数据保护人员的地位

1.在进行个人数据保护的任何相关活动时，控制者和处理者应当保证数据处理人员的参与是合适的而且及时的。

2.控制者和处理者应当对数据保护人员根据第 39 条所执行的活动予以支持（通过提供执行任务的必要资源、接触个人数据和处理机制的必要方式以及个人专业知识的培训）

3.控制者和处理者应当确保对数据保护人员不下达任何指令，他们不能因为执行任务的原因而被解雇或者受到刑事处罚。数据保护人员直接向最高管理者报告工作。和

4.数据主体可以就所有关于自身数据以及本章程规定下的自身权利问题，与数据保护人员进行联系。

5.根据联盟法律或者成员国法律，数据保护人员应当对其执行的任务内容进行保密。

6.数据保护人员也可以执行其他的任务，履行其他职责。控制者或者处理者应当确保这些执行活动不会导致利益冲突。

第 39 条 数据保护人员的任务

1.数据保护人员的任务至少包括：

（a）向控制者、处理者以及根据本章程或者根据其他联盟法律成员国法律规定的义务进行数据处理的人员，提出通知和建议。

（b）和监控本章程、其他联盟成员国法律、控制者处理者关于个人数据的相关政策（包括职责、意识提高、人员培训）以及相关审计活动的合规性；

（c）根据 35 条提出对于数据保护影响评估和监控的建议；

（d）和监管机构合作；

（e）作为监管机构与处理活动的连接点，包括 36 条提到的事先咨询或者其他咨询活动。

2.数据保护人员应当适当考虑他们的任务以及和处理机制有关的风险（考虑到处理活动的性质、范围、内容以及目的）。

第 5 章 行为法规和认证

第 40 条 行为法规

1.为了本章程得到更好地应用，成员国、监管机构、董事会和委员会应当鼓励行为法规的起草。起草应当考虑不同的处理者的具体特点，以及小微企业和中等规模企业的具体需要。

2.为了使得本法得到具体应用，协会和其他代表不同种类的主体可以为行为法规的制定、修订、扩充做准备：

（a）公平透明的处理程序；

（b）在具体情形下，控制者的立法利益；

（c）个人数据收集；

（d）个人数据的虚假信息；

（e）向公众和其他数据主体提供的信息；

（f）数据主体权利的行使；

（g）关于儿童保护以及父母抚养责任持有人同意的方式的信息收集；

（h）第 24 条和第 25 条提到的保护措施以及 32 条提到的确保安全措施；

（i）向监管机构以及其他数据主体进行个人数据泄露的通知；

（j）向第三国或者国际组织传输个人数据；

（k）根据第 77 条、第 79 条，不违背地看待数据主体权利，重视关于控制者和其他数据主体冲突解决的庭外程序以及其他冲突解决程序。

3.控制者和处理者应当制作有约束力和强制力的承诺，在保障数据主体的权利时作为保障。

4.第二款所说的行为法规应当包括使得 41 条第一款所提到的主体在进行强制监控时能够应用的守则。守则应当根据第 55 条或者第 56 条，不受监管机构权力制约，不偏不倚地得到执行。

5.本条第二款所说的协会和其他意图准备修订或者扩充现有守则的主体，应当根据第 55 条提交守则草案，修正案。监管机构应当提出草案、修正案是否符合本章程规定的意见，如果具备充分合理的保障，监管机构应当予以批准。

6.当符合第五款的草案或者修正案已经获得批准，且与成员国所进行的处理活动没有联系的时候，监管机构应当登记公开守则。

7.关于一些成员国处理活动的行为法规草案，根据第 55 条，监管机构应当在批准守则草案、修正案之前，依据 63 条的程序向董事会进行提交，而且应当附有草案、修正案是否合规的意见，根据第 3 款的情况提出合理的保障措施。

8.根据第七款的意见，提出合理的保障措施，董事会应当向委员会提交意见。

9.委员会可以通过采取措施来决定根据第八款提交的批准的行为法规、修正案在联盟内具有普遍的有效性。实施行为应当符合第 93 条第 2 款的规定。

10.委员会应当保证对符合第九款规定具有有效性的守则进行信息公开。

11.董事会会应当对行为法规、修正案进行整理和登记，并且采用合适的方式进行信息公开。

第 41 条 为法规的合法性监控

1.监管机构依据第 57 条和第 58 条的规定，不违背规定，执行任务和行使权力。可以由某个机构主体对根据第 40 条所施行的活动的加以合法性监控。

2.第一款所说的主体一种可以被认可的监督合规性主体。应当负责进行如下行为：

（a）说明它关于守则主体问题的独立性和专业性，以求获得监管机构的同意；

（b）建立能让其取得管理者和处理者评估资格的程序，对于行为合法性的加农以及对自身机制进行的阶段性复审；

（c）建立处理对违反守则或者控制者、处理者以前及现在对守则的执行情况的控告程序和结构。让程序和结构透明化和公开化；

（d）向负责的监管机构说明它的任务和职责的履行不会造成利益冲突。

3.负责的监管机构应当根据 63 条向董事会提交本条第一款所说相关主体的标准化草案。

4.第一款所提到的主体应当遵从合理的保障机制，在违反行为法规时采取合理措施，包括暂停或者排除管理者或处理者的管理权力。此外，应当将负责这些行动的相关监督主体以及行动原因进行通知。

5.如果主体行为违反或者不再满足资格，监管机构应当撤销主体资格。

6.本条不适用于公共部门和主体。

第 42 条 认证

1.出于数据保护保密标志以及说明管理者处理者处理机制合法性的需要，成员国、监管机构，委员会的董事应当尤其在联盟内激励数据保护认证机制。特别需要考量小微企业以及中等规模企业的特殊要求。

2.数据保护认证机制和根据本条第五款的密封标志可以基于说明控制者、处理者行为合理性的目的而建立。这些控制者或者处理者应当做出有约束力和强制力的承诺，包括关于数据主体的相关权利。

3.认证应当出于自愿，程序应当透明。

4.管理者、处理者的职责不能因为根据本条进行的认证而减少，必须不违背第 55 条或者第 56 条，得到监管机构的授权。

5.基于根据第 58 条第三款监管机构制定的标准或者基于根据第 63 条董事会所制定的标准，认证必须由第 43 条所提到的认证主体进行。如果标准由董事会制定，将由欧洲数据保护局来进行认证。

6.控住部门、处理者依照认证机制提交其处理过程时，应当提供 43 条所说认证主体或者负责的监管机构的信息以及具体处理活动，这些对于执行认证程序很有必要。

7.控制者、处理者的认证时间最长不超过三年，但是，如果有继续进行的需要，在相同的情况下，期间可以重新计算。当认证主体或者相关负责的监管机构不再符合条件时，认证程序将会被取消。

8.董事会应当将所有认证机制、数据保护密封标志进行整理和注册，并以任何合理的方式对公众进行公开。

第 43 条 认证主体

1.对于有关数据保护问题有一定程度经验的认证主体，在为了行使依据第 58 条获得的权力通知监管机构之后，可以公布及更新认证。成员国应当确定这些主体应当被以下至少一个机构授权：

（a）第 55 条或者第 56 条体积的监管机构；

（b）符合欧洲议会通过的 EC 第 765/2008 规定、委员会通过的 EN-ISO/IEC 17065/2012 规定以及依据第 55 条或第 56 条监管机构所制定的额外要求的国际证人主体。

2.第一款提到的认证主体只有在以下情况下才能得到授权：

（a）根据监管机构的要求，说明他们在数据主体相关问题上的独立性和经验性；

（b）承诺遵照第 42 条第 5 款提到的标准以及获得第 55 条、第 56 条或者是第 63 条所说的董事会的监管机构的认可；

（c）建立公开、阶段性复审以及取消数据保护认证，保密标志的程序；

（d）建立处理对违反守则或者控制者、处理者以前及现在对守则的执行情况的控告程序和结构。让程序和结构透明化和公开化；

（e）向负责的监管机构说明它的任务和职责的履行不会造成利益冲突。

3.第一款和第二款所提到的认证主体的授权必须基于第 55 条、第 56 条或者是第 63 条所说的董事会的监管机构的认可。在符合本条第一款所述条件下，应当根据欧洲议会通过的 EC 第 765/2008 规定以及描述认证主体认证方法和程序的技术要求，对相关要求进行补充。

4.第一款所说的认证主体应当对导致认证开始或者取消的合理的评估负责。鉴定合格最长应当在五年内进行公布，如果满足本条所列条件，在相同的情况下，期间可以重新起算。

5.第一款所说的数据主体应当向监管机构提供准予认证和撤销认证的理由。

6.第三款所说的要求以及第 42 条第 5 款所说的标准应当以一种简便的方式向公众公开。监管机构也应当向董事会传达具体要求和标准。董事会应当将所有认证机制、数据保护密封标志进行整理和注册，并以任何合理的方式对公众进行公开。

7.遵照第八章的规定，负责的监管机构或者国际鉴定主体在认证主体的行为违反规定或者认证条件不满足或者不再满足的情况下，应当撤销认证。

8.委员会应当被授权依据第 92 条，为了实现具体化认证要求的目的，来采取一些被授权进行的行动（考虑到第 42 条第一款所提到的数据保护认证机制）

9.委员会可以采取措施规定认证机制和数据保护密封标志的技术性标准。行动应当根据第 93 条第 2 款的规定进行实施。