一般数据保护法

（General Data Protection Regulation）

全文译文

译制工作组：高志民、张大伟、高强裔、居崑、陈聪、

卢倩倩、白阳、刘吉强、银鹰

国家金融 IC 卡安全检测中心信息安全实验室

北京交通大学金融信息安全研究所

上海交通大学网络空间安全学院

2018 年 3 月 30 日

《一般数据保护法案》

General Data Protection Regulation

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

第一章. 总则

第 1 条 主题与目标

1 该法规制定了在处理个人资料方面保护自然人的规则，及与个人资料自由流动有关的规则。

2 本法规保护自然人的基本权利和自由，尤其是自然人保护其个人资料的权利。

3 不得以保护与个人数据处理相关的自然人为由，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 本法规完全或部分适用于以自动方式对个人数据的处理，除了以自动方式处理构成或拟构成档案系统一部分的个人资料。

2 本法不适用于以下个人数据的处理：

a) 在一项不属于欧盟法律范围活动的过程中;

b) 成员国在开展属于"欧盟条约(TEU, the Treaty on European Union)"第五卷第 2 章范围内的活动时;

c) 自然人在纯粹的个人或家庭活动中;

d) 由主管当局以预防、调查、侦查或起诉刑事犯罪为目的；或执行的刑事处罚，包括防范和防止对公共安全的威胁。

3 欧盟各机构、机关、办事处和专门行政部门（代理机构）处理个人数据，适用第 45/2001 号法规。第 45/2001 号法规和其他适用于处理个人资料的欧盟法律应根据本法规第 98 条的规定对其进行调整。

4 本法规不影响第 2000/31/EC 指令的适用，特别是该指令第 12 条至第 15

条对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费用；或

b) 是对数据主体发生在欧盟内行为的监控。

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

为了达到本法规目的：

1 "个人资料"是指与一个确定的或可识别的自然人相关的任何信息（数据对象）。可识别的自然人指可以直接或间接识别的人，特别是通过参考诸如姓名、身份证号码、位置数据、在线身份识别等标识符，或参考与该自然人的身体、生理、遗传、心理、经济、文化或社会身份有关的一个或多个因素。

2 "处理"是指针对个人数据或个人数据集合的单一操作或一系列操作，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、传播或以其他方式应用，排列、组合、限制、删除或销毁，无论此操作是否采用自动化手段。

3 "限制处理"是指对储存的个人资料作标记，以限制日后的处理。

4 "特征分析"是指任何对个人数据进行的自动处理，包括利用个人数据对自然人的某些个人方面的评估，特别是对自然人在工作、经济状况、健康、个人喜好、兴趣、可靠性、行为、地点或流动性等方面的分析或预测。

5 "匿名化"是一种处理个人资料的方式，即不使用额外信息便不能将个人资料归于某一特定资料主题，该处理方式需将额外信息分开存储，并施加技术和组织措施，以确保个人资料不属于已识别或可识别的自然人。

6 "整理汇集系统"是一种依照特定标准，无论集中、分散（基于功能或地理基础上的分散）都可访问的任意结构化个人数据。

7 "控制者"是能单独或联合决定个人数据处理目的和处理方式的自然人、法人、公共机构、行政机关或其他非法人组织。其中个人数据处理目的和方式，以及控制者或控制者提名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"是指代表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"是指被披露个人数据的接收者，无论其是否是第三方自然人、法人、公共机构、行政机关或其他非法人组织。政府当局在欧盟或其成员国法律框架内的特定调查接收到个人数据时，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"是指自然人或法人、政府当局、机构或除了数据主体的机构、控制者、处理者，以及在控制者或处理者直接授权下有权处理个人数据的人。

11 对数据主体的"同意"是指任何自由、具体、知情和毫不含糊地表示数据主体意愿的行为，通过声明或明确的肯定行动表示同意处理与其有关的个人数据。

12 "个人数据外泄"是指引起了意外或非法毁坏、遗失、更改、未经授权披露或访问传输、存储或正在处理的个人数据的安全破坏行为。

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技术处理后得到的个人数据。这类数据生成了该自然人的唯一标识，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，包括能揭示关于其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，在本法规下承担特定义务；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场所，在本法规下承担特定义务。

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 "具有约束力的公司规则"是指在成员国领土上设立的控制者或处理者遵守的个人数据保护政策，以便将个人数据转让给企业集团内一个或多个第三国的控制者或处理者，或从事联合经济活动的企业集团。

21 "监督机构"是指一个独立的，由成员国依据第 51 条设立的独立公共权利机构。

22 "有关监督机构"指与个人数据处理有关的监督机构，因为:

a) 控制者或处理者是设立在监督机构所在的成员国领土上的；

b) 居住在监督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) 一个由监督机构提交的申诉。

23 "跨境处理"是指以下情形之一：

a) 个人数据处理发生在设立在欧盟中的多个成员国内的控制者或处理者在多个成员国内的营业机构的活动中。

b) 个人数据处理发生在一个欧盟内的控制者或处理者唯一营业机构的活动中，但是这种处理可能或会严重影响多个成员国的数据主体。

24 "相关且合理异议"是指一种关于是否存在违反本法情况，或控制者、处

理者是否存在遵守本法预设行为的异议。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风险的重要影响，同时此种异议也适用于欧盟内个人数据的自由流动。

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) 以与数据主体有关的，合法、公正、透明的方式处理（"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，且不得以不符合以上目的的方式进行进一步处理；为公共利益、科学、历史研究或统计目的而进一步处理的，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必要性为限度进行处理（"数据最小化"）；

d) 准确，并在必要时保持最新；考虑到处理个人数据的目的，必须采取一切合理的措施，毫不拖延地删除或纠正不准确的个人资料("准确性")；

e) 个人数据需以容许资料主题被识别的形式，在不超过处理个人资料所需的时间内保存；个人数据可以储存更长时间，只要个人数据按照第 89 条第(1)款规定，仅为公众利益、科学、历史研究或统计目的而进行处理，但须执行本法规所要求的适当技术和组织措施，以保障数据主体的权利和自由("储存限制")；

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避免未经授权、非法处理、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，处理才被视为合法：

a) 数据主体同意其个人数据为一个或多个特定目的而处理;

b) 处理是为履行数据主体参与合同的必要行为，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) 为了控制人或第三方所追求的合法利益，处理是必要的，除非这种利益与保护个人数据的数据主体利益或基本权利和自由相冲突，特别是在数据主体是儿童的情况下。该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条款的应用，以遵守第一款的(c)项和(e)项，更准确地确定处理的具体要求和其他措施，以确保处理的合法和公平，包括第九章规定的其他具体处理情况。

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。

处理的目的须由该法律基础决定，或者根据第一款（e）项中所指的处理，即应当为了执行必要的、为了公共利益的任务或行使控制者被赋予的官方权力而进行的工作。法律依据可以包括具体条款以此来适应本法规条款的应用，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及其目的、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合法目标相称。

4 为收集个人资料以外的目的而进行的处理，并且这个目的不是基于数据

主体的同意，亦非民主社会中的一个构成必要或适当措施来保障第 23 条（1）款中提到的欧盟或成员国法律，控制者应当考虑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一致，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，特别是是否是依据第 9 条处理的特殊类别的个人数据，或是否是依据第 10 条与刑事定罪和犯罪有关的个人数据；

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 同意的条件

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其个人数据。

2 如数据主体通过书面声明的方式做出同意，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其同意。同意的撤回不应影响在撤回前基于同意做出的合法数据处理。在做出同意前，数据主体应被告知上述权利。撤回同意应与做出同意拥有同样的难易度。

4 当评估同意是否是自由做出时，应尽最大可能考虑到：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，处理只有在获得儿童父母责任（parental responsibility）持有者的同意或授权时才合法。会员国可通过法律规定较低年龄，但此种较低年龄不得低于 13 岁。

2 考虑到现有技术，控制者应当做出合理的努力，去核实在此种情况下，儿童的父母责任持有人是否同意或授权。

3 第 1 款不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、宗教或哲学信仰以及工会成员的个人数据处理，以及对以唯一识别自然人为目的的基因数据、生物特征数据，自然人的健康、性生活或性取向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) 数据处理为达到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、行使权利的目的的处理是必要，但应由欧盟或会员国法律或集体协议授权，根据会员国法律，为数据主体的基本权利和利益提供适当的保障；

c) 为了保护数据主体或另一个在物理或法律上无法给出同意的自然人的重大利益时，处理是必要的；

d) 数据处理是由以政治、哲学、宗教、工会为目的的协会、组织或其他任何非营利机构在有适当安全保障的合法活动中进行的，处理应当仅涉及该组织的成员或前成员，或与该组织的宗旨有经常接触的人，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) 数据处理是为合法诉求的成立、行使或辩护所必须的，也是在法院以其司法身份行事时所必需的；

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) 为了预防或职业医学的目的，为了评估雇员的工作能力、医疗诊断、提供保健或社会护理或治疗，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，并在第 3 段所述条件和保障措施的基础上管理保健或社会护理系统和服务时，数据处理是必要的；

i) 在公共健康的领域为了公共利益的考虑，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，依据欧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) 根据欧盟或成员国法律，为了公众利益、科学、历史研究或统计目的的处理工作是必要的，这些目的应与其所追求的目标相称，尊重数据保护权的实质，并规定适当和具体的措施以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由负有保守专业秘密义务的专业人士处理，或者在其负责下处理；或者由另一个同样依据欧盟或其成员国法律或国家法定机构规则，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

根据第 6 条第(1)款处理与刑事定罪和犯罪有关的个人资料或相关的安全措施时，只有在官方当局控制下或在联邦或成员国法律授权的情况下才能进行，这些法律规定了对数据主体的权利和自由的适度保障。任何全面的刑事定罪登记都只应在官方权力的控制下保存。

第 11 条　无需识别的处理

1 如控制者为实现处理个人资料的目的不需要或不再需要控制者控制的识别资料，则控制者无须纯粹为遵从本规例而备存、取得或处理额外资料以识别该等资料。

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，说明自己不需要对数据主体进行识别。在这种情况下，第 15 条至第 20 条不适用，除非数据主体为行使这些条款规定的权利而提供更多信息，以便识别其身份。

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中的沟通信息（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以及向监督机构提起申诉以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，尤其是重复提出要求的情形下，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 欧洲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信息和程序的权利。

第二节. 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 1 款的规定进行时，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收方的种类；

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、欧洲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 2 分款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) 如果处理是基于第 6 条第(1)款(A)点或第 9 条第(2)款(A)点，则在任

何时候存在撤回同意的权利，而不影响撤回前基于同意的处理的合法性；

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、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关于可能造成的后果的信息；

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，适当时还要提供其代表人的信息；

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、欧洲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) 如果处理是基于第 6 条第(1)款(A)点或第 9 条第(2)款(A)点，则在任何时候存在撤回同意的权利，而不影响撤回前基于该同意的处理的合法性；

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) 如果个人数据将用于与该数据主体进行通信，最迟应在第一次通信时按规定提供信息；

c) 如果计划向另一收件人披露个人资料，最迟在第一次披露个人资料时按规定提供信息。

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或将涉及不成比例的努力，特别是为了公众利益、科学或历史研究或统计目的而进行的处理，但须符合第八十九条第一款所述的条件和保障措施，或在本条第一款所述义务可能使使这一处理的目标无法实现或严重损害目标的实现。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) 控制者应当根据欧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) 根据欧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

1 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获得以下信息：

a) 处理的目的；

b) 有关个人数据的类别；

c) 个人数据已被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) 在可能的情况下提供预期的个人数据保留时间；或者不可能时提供用于确定该保留时间的标准；

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) 向监督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的意义和预期的后果。

2 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。

3 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信息，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。

4 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。

第三节. 纠正和删除

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与其相关的不准确个人数据。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 删除权（被遗忘权）

1 数据主体有权要求控制者无不当延误地删除与其有关的个人数据，并且根据下列任意理由，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（数据）处理相关法律依据的情况下；

c) 数据主体根据第 21 条第 1 款反对处理，并且没有相关（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) 个人资料须予删除，以符合控制者所遵守的欧盟或成员国法律所规定的法律义务；

f) 收集的个人资料涉及第 8 条第 1 款所述的提供的社会服务信息。

2 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。

3 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欧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的任务；

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；

d) 根据第 89 条第 1 款，为了公共利益、科学或历史研究或统计目的，就第 1 款所述的权利可能使该处理的目标无法实现或严重损害其实现；

e) 为了设立、行使或捍卫合法权利。

第 18 条　限制处理权

1 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质疑，且允许控制者在一定期限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，同时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 款反对该处理。

2 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，或为了欧盟或成员国的重要公共利益的原因被处理。

3 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。如果数据主体对此提出请求，控制者应当将这些接收者通知数据主体。

第 20 条　数据可移植性权利

1 数据主体有权以结构化、通用和机器可读的格式接收其提供给控制者的与其有关个人数据，当满足以下任意条件时，数据主体有权将这些数据不受提供该个人信息的控制者阻碍地传输给另一个控制者：

a) 处理是根据第 6 条第 1 款第(a)项或第 9(2)条第 2 款第(a)项，又或根据第 6 条第 1 款第(b)项的同意；以及

b) 采用自动化方法进行处理。

2 根据第 1 款行使其数据可移植性权利时，在技术可行的前提下，数据主体有权将个人数据直接从一个控制者传输给另一个控制者。

3 本条第 1 款所述权利的行使，不影响第 17 条。该权利不适用于为公共利益所执行的一项任务所必需的处理，也不适用于行使由控制者指派的官方职权（职务权限）。

4 第 1 款所指的权利不得对他人的权利和自由产生不利影响。

第四节. 拒绝权和自主决定权

第 21 条 拒绝权

1 数据主体应有权在任何时候以与其具体情况有关的理由，反对根据第 6 条第(1)款(E)或(F)点处理与其有关的个人数据，包括基于这些规定的特征分析。除非控制者有令人信服的合法理由证明其可以处理凌驾于数据主体的利益、权利和自由之上的信息，或提出、行使或辩护合法的申索，否则控制者不得再处理该等个人资料。

2 如果个人数据是为直接营销目的进行的处理，数据主体应有权在任何时候反对处理与其本人有关的个人数据，来进行这种营销，包括在与这种直接营销有关的范围内进行的分析。

3 数据对象为了直接营销目的而进行处理的，不得再为该目的处理个人资料。至少在与数据主体第一次沟通时，应明确请数据主体注意第 1 和第 2 款所述权利，并应与其他任何相关信息清楚地分开呈现。

4 在信息社会服务使用的背景下，即使有欧盟 2002 年的指令，数据主体仍可通过使用技术规范的自动化方式行使其拒绝权。

5 第 89 条第 1 款所述个人数据因科学或历史研究或统计的目的被处理的，数据主体在与其相关的特定情形下，有权拒绝对其个人数据的处理，除非这种处理对于因公众利益而执行的任务是必要的。

第 22 条 个人决策自动化，包括分析

1 数据主体有权不受完全基于自动处理的决定的约束，包括对其产生的法

律效果或类似重大影响的分析。

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) 控制者是数据主体的情况，按照欧盟或成员国的法律的规定，应确立适当的措施，以维护数据主体权利、自由和正当利益；或

c) 由数据主体明确同意的。

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维护数据主体的权利、自由和正当利益，至少有权获得对控制者的干预，表达其观点并对决定提出异议。

4 第2款所指的决定不得以第9条第1款所述的特殊类别个人数据为依据，除非适用第 9 条第 2 款的第（a）或（g）项，且采取适当的措施以保护数据主体的权利、自由和正当化利益。

第五节. 限制

第 23 条 限制

1 欧盟或成员国法律规定，主体是数据控制者或处理者，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 条与第 12 条至 22 条相对应的权利和义务。这种限制尊重了基本权利和自由的本质，是民主社会必要且适当的措施，以此维护：

a) 国家安全；

b) 防务；

c) 公共安全；

d) 刑事犯罪的预防、调查、侦查或起诉，或执行刑事处罚，包括对公共安全威胁的预防和防范；

e) 欧盟或一个成员国一般公共利益的其他重要目标，特别是欧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) 预防、调查、侦查和起诉受管制职业的违反道德行为；；

h) (A)至(E)和(G)项所述情况下与行使官方权力有关（包括偶尔相关）的监测、检查或管理职能；

i) 对数据主体的保护或对其他人的权利与自由的保护；

j) 对民事诉讼主张的强制执行。

2 特别是，在第 1 款所指的任何立法措施，应至少包含有关如下内容的具体规定，如：

a) 处理或分类的目的；

b) 个人数据的分类；

c) 引入的限制范围；

d) 防止滥用、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的类别；

f) 加工或加工类别的性质、范围和目的及其存储期限和适用的保障措施；

g) 数据主体的权利和自由所面临的风险；以及

h) 数据主体对限制的知情权，除非有损于限制的目的。

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 考虑到处理的性质、范围、内容和处理的目的以及自然人的权利和自由由于可能性和严重性不断变化所带来的风险，控制者应当实施适当的技术和组织措施，以确保并能够证明处理是根据本法规进行的。这些措施应在必要时加以审查和更新。

2 与有关处理活动相称的情况下，第 1 款所指的措施应包括由控制者执行的数据保护政策。

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，用以证实控制者的义务遵守情况。

第 25 条　设计和默认的数据保护

1　考虑到处理的性质、范围、内容和处理的目的以及自然人的权利和自由由于可能性和严重性不断变化所带来的风险，控制者应该在确定处理手段和处理本身的同时，实施适当的技术和组织措施，如匿名化，其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访问性。特别是，这些措施应确保在没有个人对不定数目自然人的干预下，个人数据是不可访问的。

3　根据第 42 条的经批准的认证机制可以作为一个元素，以证实对本条第 1 款和第 2 款要求的遵守。

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，除非控制者各自的责任由欧盟或成员国法律确定。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联合控制者相对于数据主体的各自作用和关系。数据主体应能够获知该安排的实质。

3　不论在第 1 款所指的安排条款为何，数据主体可以根据本法案对每一名管制员行使其权利。

第 27 条　未在欧盟中设立的控制者或处理者的代理人

1　适用第 3 条第 2 款，控制者或处理者应当以书面形式指定欧盟中的代理人。

2　本条第一款中的义务不适用于：

a)　偶然的处理，不包括大规模处理第 9 条第 1 款提及的特殊类别的数据处理，也不包括第 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

可能对自然人的权利和自由造成危害；或者

b) 一个公共权力机关或机构。

3 代理人应当被设立在一个成员国中，其数据主体为其个人数据，其个人数据涉及向其提供产品或服务，或者其行为受到监控。

4 为确保遵守本法规的目的，代理人应获得控制者或处理者的授权，以及特别是监督机构和数据主体的授权，以处理所有的相关问题。

5 控制者或处理者对代理人的指定，应不违背由控制者或处理者自身发起的合法行为。

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案的要求，确保对数据主体权利的保护。

2 如果事先未经处理者特别的或一般的书面授权，该处理者不能引入另一个处理者参与处理。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处理者的变化，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欧盟或成员国法律下的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，个人数据的类型、数据主体的类别和控制者的权利义务。该合同或其他法律行为应规定，特别是对处理者规定以下几点：

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某一第三国家或国际组织的转移，除非处理者所遵守的欧盟或成员国法律允许非书面指示的做法，其中该处理者是主体；在这种情况下，处理者在处理之前，应通知控制者相关的法律要求，除非法律由于重大公共利益原因禁止提供这样的信息；

b) 确保被授权处理个人数据的个人，已承诺保密或在适当的法定保密义务下；

c) 采取第 32 条要求的所有措施；

d) 遵从第 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，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，在提供有关处理服务的最后，就需要删除或向该控制者返还所有的个人数据，并删除现有的复制版本，除非欧盟或成员国法律要求存储其个人数据；

h) 使控制者能够获取所有必要的信息，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，该审计和检查过程是由控制者或由控制者授权的另一审计员执行的。

关于第一分款的第 h 项，如果在其看来，一个指令违反了本法规或其他欧盟或成员国的数据保护规定，处理者应当立即通知控制者。

4 处理者引入其他处理者执行代表控制者的特定处理活动的，参照第 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要求，应通过欧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，确保处理能满足本法案要求。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 处理者遵守第四十条所指的经核准的行为守则或第四十二条所指的经核准的认证机制，可用作证明本条第 1 款和第 4 款所述充分保证的要素。

6 在不损害控制者和处理者之间的个人合同前提下，在本条第 3 款和第 4 款提及的合同或其他法律行为，可全部或部分以本条第 7 和第 8 款所指的标准合同条款为依据，包括在这些条款是根据第 42 条和第 43 条给予控制人或处理者的证明的一部分时。

7 欧洲委员会可就本条第 3 款和第 4 款所指的事项制定标准化的合同条款，并与第 93 条第 2 款所指的审查程序保持一致。

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，应当以书面形式给出，包括电子形式。

10 在不损害第 82 条、83 条和 84 条的情况下，如果一个处理者因决定处理的目的和手段违反了本法案的规定，该处理者可以在该处理过程中被认为是控制者。

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该个人数据，除非欧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，以及适用情况下的控制者的代理人，应当依其职责保存处理活动的记录。该记录应当包括以下所有信息：

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

b) 处理的目的；

c) 数据主体类别和个人数据类别的描述；

d) 个人数据已经或将要被公开的收件人的类别，包括位于第三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 2 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 款提及的技术和组织安全措施进行一般性描述。

2 每一个处理者，以及在适用情况下的处理者的代表，应保存代表控制者执行的所有处理活动类别的记录，其中包括：

a) 处理者的名称和联系方式，以及代表其行为的每个控制者的名称和联系方式，以及在适用的情况下，控制者或处理者的代表以及数据保护专员的名称和联系方式；

b) 代表各控制者进行的处理类别；

c) 在适用的情况下，将个人数据向第三国或国际组织的转移，包括第

三国或国际组织的确定，以及在第 2 分款第 49 条第 1 款所指的转移情况下的，适当保障措施的文件；

d) 在可能情况下，对第 32 条第 1 款所述的技术和组织安全措施进行一般性说明。

3 第 1 和第 2 款所述的记录应以书面形式呈现，包括电子版本。

4 控制者或处理者，以及在适用情况下的控制者或处理者的代表，应按要求将记录提供给监督机构。

5 第 1 款和第 2 款中所指的义务不适用于雇员少于 250 人的企业或组织，除非它执行的处理可能为数据主体的权利和自由带来风险的，该处理是非偶然的，或该处理包括特殊数据类别的，即第 9 条第 1 款所指数据，或第 10 条所指刑事定罪和犯罪相关个人数据。

第 31 条　和监督机构的合作

执行任务的过程中，控制者、处理者以及使用情况下的它们的代表，应当根据要求与监督机构进行合作。

第二节. 个人数据安全

第 32 条　处理过程的安全性

1 考虑目前的工艺水平、实施成本、处理过程的性质、范围、目的，以及自然人自由和权利所面对的不同可能性和严重性风险，控制者、处理者应当执行适当的技术和组织措施来保证合理应对风险的安全级别，尤其要酌定考虑以下因素：

a) 个人数据的匿名化和加密；

b) 确保处理系统和服务现行的保密性、完整性、可用性以及可恢复性；

c) 在发生物理事故或技术事故的情况下，恢复可用性以及及时获取个人信息的能力；

d) 定期对技术措施以及组织措施的有效性进行测试、评估、评价处理，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，特别是抵御对个人数据的意外和非法销毁、损失、变更、未经授权披露，或是对个人数据的传送、存储或其他处理过程中的风险问题。

3 参考第 40 条批准的合法行为或者参考第 42 条通过的认证机制，均可用来证明本条第 1 款要求的合规性。

4 控制者以及处理者应当逐步采取措施，以求控制者和处理者管辖下、能够访问个人数据的自然人不能对这些数据进行处理，除非获得控制者的指示，或者其应欧盟或成员国法律的要求而进行处理时。

第 33 条　监督机构对个人数据泄露的通知

1 在个人数据泄露的情况下，控制者应毫不延误地，且在可行的情况下，应至少在获知之时起 72 小时以内，依据第 55 条通知监督机构，除非个人数据的泄露不会产生危及自然人权利和自由的风险。如果通知迟于 72 小时，须附述迟延原因。

2 一旦发现信息泄露，处理者应当毫不延误地通知控制者。

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，尽可能地包括相关数据主体以及个人数据记录的类别和大致数量；

b) 交流数据保护专员或其他能够获取更多信息的联系点的名称和联系方式；

c) 描述个人信息泄露的可能情况；

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

4 在目前为止不可能同时提供信息的情况下，应毫无进一步不当延迟的情况下，对信息进行分阶段提供。

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，这些能够便于监督机构对行为合规性进行核查。

第 34 条　关于数据主体的个人数据交流

1 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的泄露与数据主体进行交流。

2 本条第一款提到的数据主体交流，至少应当包括第 33 条第 3 款的（b）（c）（d）三项所涉及的信息和建议，并用清晰且平实的语言描述个人

数据泄露的性质。

3 以下这些情况下，不能适用第 1 款所提到的数据主体交流：

a) 控制者已经采取适当的技术及组织保护措施，而且此类措施已经被应用于受到信息泄露影响的个人数据之中，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) 控制者已经采取后续措施，这些措施能够确保第一款所指数据主体的权利和自由的高度风险不可能实现的。

c) 这会涉及到不成比例的努力。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。

4 如果控制者并未就个人数据泄露与数据主体进行交流，考虑到个人数据信息泄露可能带来的高度风险，监督机构可以要求其这样做或者可以决定其依据第 3 款所提任何条件。

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，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。单一评估可能对一组具有类似高风险的操作进行处理。

2 当进行数据保护影响评估时，受委任的控制者可以向指定的数据保护专员寻求帮助。

3 以下情形尤其适用于第 1 款所说的数据保护影响评估：

a) 对自然人个人情况评估所进行的系统和广义上的评估也是基于自动处理过程，包括分析，以及基于哪些决定会对自然人产生法律效力或对自然人产生同样重大的影响；

b) 第 9 条第 1 款提到的大范围的数据处理或者第 10 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 1 款，建立并公布一套数据处理机制，使其符合数

据保护影响评估的要求。监督机构应当就此与第 68 条所提到的理事会进行交流。

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。监督机构应当就该列表与理事会进行交流。

6 在采取第 4 款和第 5 款的措施之前，监督机构应当应用第 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移动相关的处理活动。

7 该评估至少应包括以下内容：

a) 对于所设想机制以及处理目的（包括数据应用、控制者所追求的合法利益）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和自由的风险评估；

d) 所设想的处理风险的举措，包括保障措施、安全措施、确保个人数据保护的机制，以及考虑到数据主体权利和合法利益的，用于证明对于本法案的合规性的举措。

8 在评估处理机制影响的过程中，对于第 40 条所规定的相关控制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 适当情况下，控制者应当寻求数据主体或者其在预期处理方面的代表的观点，且不危害商业和公共利益的保护或者处理机制的安全。

10 第 6 条第 1 款（c）项或（e）项所述处理，依据欧盟法律或者成员国法律，控制者是主体，这些法律规定了具体的处理操作或者相关操作集。数据保护影响评估方式已被当作是一般影响评估的一个部分得到实施。其中，第 1 款到第 7 款不能适用，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决定的，在处理机制的风险出现变化的时候，控制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 监察当局认为第 1 款所指的处理程序会违反本规例的，特别是控制者未充分识别或减轻风险的，监督机构应当最迟在接到咨询请求的 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 6 周。监督机构应当将此类延期在接到咨询请求的一个月内，连同迟延理由，通知控制者，并在适用情况下通知处理者。直到监督机构实现它所要求的咨询目的，这些期间将可被终止。

3 根据第一款向监督机构咨询时候，控制者应当向监督机构提供：

a) 适用情况下，控制者，连同处理相关的控制者和处理者的相关职责，尤其是企业团体内的处理过程的；

b) 预期处理的目的和手段；

c) 根据本法保护数据主体权利和自由的保障措施；

d) 适用情况下，数据保护局的联系方式；

e) 第 35 条所规定的数据保护影响评估；以及

f) 监督机构所要求的其他信息。

4 成员国应当在准备方案期间向监督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，对于涉及公共利益的、包括社会保护和公众健康的处理程序，应当获得监督机构的预先授权。

第四节. 数据保护专员

第 37 条 数据保护专员的指派

1 在以下情况下，控制者和处理者应当指派数据保护专员：

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，因其本质性质、范围和/或目的所决定的，需要对数据主体进行定期和系统的大规模监控的；或者

c) 由第9条所述大规模特殊种类数据和第10条所述刑事定罪和犯罪相关个人数据的处理所组成的控制者或处理者的核心活动；

2 企业团体可以任命一个独立的数据保护专员，前提是每个机构都能很容易地联系到该数据保护专员。

3 控制者或处理者是某一公共机关或机构的，考虑到它们的组织结构和规模，可为几个这样的机构或机构指定一个数据保护官员。

4 除了第一款所涉及的情况，控制者、处理者、协会和其他代表不同种类控制者和处理者的机构，或者据欧盟或者成员国法律所设立的部门，应当指派数据保护专员。数据保护专员可为这些机构以及代表控制者或处理者进行活动。

5 数据保护专员的指派应当基于专业资质，且特别是关于数据保护法律的专业知识以及第 39 条所指的完成任务的经验和能力。

6 数据保护专员可以是控制者或处理者的成员，或在服务合同的基础上完成任务。

7 控制者或处理者应当公布数据保护专员的联系方式，并且将名单告知监督机构。

第 38 条　数据保护专员的地位

1 在进行任何个人数据保护的相关活动时，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专员根据第 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、获取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专员不接受关于行使职能的任何指示，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。数据保护专员直接向最高控制者报告工作。以及：

4 数据主体可以就所有关于自身数据以及本法规规定下的自身权利问题，与数据保护专员进行联系。

5 根据欧盟法律或者成员国法律，数据保护专员应当对其执行的任务内容进行保密。

6 数据保护专员也可以履行其他的任务和职责。控制者或处理者应当确保

该过程不会导致利益冲突。

第 39 条　数据保护专员的任务

1　数据保护专员的任务至少包括：

a) 向控制者、处理者以及根据本法规或者根据其他欧盟法律或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) 监测本法规、其他欧盟或成员国数据保护法律条款，以及控制者或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) 根据第 35 条提出对于数据保护影响评估和监控的建议；

d) 和监督机构合作；

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

2　考虑到处理活动的性质、范围、内容以及目的，数据保护专员应当适当考虑他们和处理操作有关联的有关风险的执行。

第五节.　行为准则和认证

第 40 条　行为准则

1　为了本法规得到更好地应用，成员国、监督机构、理事会和欧洲委员会应当鼓励行为准则的起草。该准则的起草应当考虑不同的处理者的具体特点，以及微、小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准则的制定、修订或扩充做准备：

a) 公平透明的处理程序；

b) 在具体情形下，控制者的合法利益；

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) 关于儿童保护以及在父母抚养责任持有人同意的前提收集信息；

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

i) 向监督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 除了控制者或处理者对本法案的依存性，按照本条第 5 款通过的行为准则，以及根据本条第 9 款所赋予的一般效力，根据第 3 条不服从本法的控制者和处理者也同样依从。根据第 3 条不服从本法的目的在于在第 46 条第 2 款(e)项所述框架内的个人资料向第三国或国际组织的转移提供适当的保障措施。这些控制者和处理者应通过合同或其他具有法律约束力的文书，形成具有约束力和可执行性的承诺，以应用于包括有关数据主体权利在内的适当保障措施。

4 第二款所说的行为准则应当包括使得第 41 条第 1 款所提到的主体在对合规性进行强制监控时能够应用的准则。准则应当不受监督机构权力制约，且职责和权利的履行不违背第 55 条或者第 56 条所述监管机构职能。

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准则的主体，应当根据第 55 条向监督机构提交准则草案、修正案及扩充案。监督机构应当就其是否符合本法规定提出意见，且如其具备充分合理的保障机制，监督机构应当予以批准。

6 当符合第 5 款的草案、修正案或扩充案已获得批准，且与成员国所进行的处理活动没有联系时，监督机构应当登记并公开该准则。

7 关于一些成员国处理活动的行为准则草案，根据第 55 条，监督机构应当在批准准则草案、修正案或扩充案之前，将其依据 63 条的程序提交给理事会，而且应当附有草案、修正案或扩充案是否符合本法的意见，在第 3 款所述情况下，还应提供合理的保障措施。

8 根据第七款所得意见，确认草案、修正案或扩充案符合本法规，或在第 3 款所述情况下，提供合理的保障措施的，理事会应当向欧洲委员会提交意见。

9 欧洲委员会可以通过采取措施来决定根据第 8 款提交的行为准则、修正案或扩充案在欧盟内具有普遍的有效性。其实施行为应当符合第 93 条第 2 款的规定。

10 欧洲委员会应当确保对符合第 9 款规定的具有有效性的准则进行信息公开。

11 理事会应当对行为准则、修正案或扩充案进行整理和登记，并且采用适当的方式进行公开。

第 41 条　行为准则的合法性监控

1 监督机构依据第 57 条和第 58 条，在不违背所规定的监督机构职责和任务的情况下，根据第 40 条对行为准则合规性地进行监控，可以由某个机构来实现，该机构应达到与该准则主题相关适当专家的水平，且就此目的得到主管监督机构认定的。

2 第 1 款所说的主体可以得到认定，用以监控行为准则的合规性，该机构应：

a) 证明它关于准则主题问题的独立性和专业性，以求获得监督机构的同意；

b) 建立能让其取得控制者和处理者评估资格的程序，对于行为合法性的监控以及对自身条款进行阶段性的复查；

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

d) 向负责的监督机构证明它的任务和对职责的履行不会造成利益冲突。

3 负责的监督机构应当根据第 63 条向理事会提交本条第 1 款所说相关主体的标准化草案。

4 在不影响主管监督当局的任务和权力以及第八章规定的情况下，本条第 1 款所述机构应在适当保障措施的限制下，对控制者或处理者违反守则的情况采取适当行动，包括暂停或排除有关控制者或处理者的行为，应向主管监督机关通报这些行动及其理由。

5 如果机构行为违反或者不再满足资格，监督机构应当撤销机构资格。

6 本条不适用于公共机关和机构。

第 42 条　认证

1　成员国、监督当局、理事会和委员会应特别鼓励在欧盟一级建立数据保护认证机制和数据保护印鉴和标记，以表明控制者和处理者遵守本法规的规定，微、小企业以及中等规模企业的特殊要求也应加以考量。

2　除受本规则管制的控制者和处理者遵守外，可建立根据本条第五款核准的数据保护认证机制和数据保护印鉴或标识，证明控制者、处理者提供了适当的保障措施，这些措施是第 46(2)条(F)项所述条件下的向第三国或国际组织转让个人资料的框架内，不受本法规第 3 条的约束。

3　认证应当出于自愿，并通过透明的程序提供。

4　根据本条进行的认证不会减少控制者或处理者遵守本法规的责任，也不影响监督机构根据第 55 条或第 56 条所规定的任务和权力。

5　本条规定的证明应由第四十三条所指的验证机构或主管监督当局根据该主管监督当局根据第五十八条第三款核准的标准或欧盟根据第六十三条核准的标准颁发。如果标准得到欧盟的批准，这可能会产生一个共同认证，即欧洲数据保护印章(European Data Protection Seal)。

6　向认证机制提交其处理程序的控制者或处理者应提供第四十三条所指的认证机构，或在适当情况下向主管监督当局提供进行认证程序所必需的一切信息和对其处理活动的访问权。

7　控制者、处理者的认证时间最长不超过三年，并可在相同条件下延长，但须继续满足有关要求。当该认证相关的要求不再被满足时，该认证将由第 43 条所指的认证机构或相关负责的监督机构撤销。

8　理事会应收集所有认证机制、注册在内的数据印鉴和标识，并以适当的方式对公众公开。

第 43 条　认证机构

1　在不影响第五十七条和第五十八条规定的主管监督当局的任务和权力的情况下，在数据保护方面具有适当水平专门知识的验证机构在通知监督当局以便使其能够根据第五十八条第(2)款行使其权力之后，应在必要时签发和续签证书。成员国应当确定这些验证机构应当被以下至少一个机构授权：

a)　第 55 条或者第 56 条提及的监督机构；

b) 符合欧洲议会通过第 765/2008 规定、欧洲委员会通过的 EN-ISO/IEC 17065/2012 规定以及依据第 55 条或第 56 条由监督机构所制定的额外要求的国家认证机构。

2 第 1 款提到的认证机构只有在以下情况下才能得到授权：

a) 根据监督机构的要求，说明他们在认证主题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 条所说的理事会的监督机构的认可；

c) 建立公开、阶段性复审以及取消数据保护认证，印鉴和标识的程序；

d) 建立程序和结构，以处理关于违反认证，控制者或处理者实施或正在实施认证的方式的投诉，并使这些程序和结构对数据主体和公众透明；

e) 向负责的监督机构证明其要求已满足，其任务和职责的履行不会造成利益冲突。

3 第 1 款和第 2 款所提到的认证机构的授权应根据基于第 55 条或第 56 条行事的监督当局或理事会根据第 63 条核准的标准进行。在符合本条第 1 款所述条件下，应当根据欧洲议会通过的第 765/2008 规定以及其描述认证机构的认证方法和程序的技术要求，对相关要求进行补充。

4 第 1 款所指认证机构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 第一款所说的认证机构应当向监督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。监督机构也应当向理事会传达具体要求和标准。理事会应当将所有认证机制、注册的数据保护印鉴和标识进行收集，并以合理的方式对公众进行公开。

7 在不妨碍第八章的情况下，被认可的认证机构的条件不符合或不再符合规定，或者认证机构采取的行动违反本法规时，主管监督机构或国家认可机构应撤销对本节第 1 款所规定的认证机构的认可。

8 授权委员会应根据第 92 条采取授权行为，以具体说明第 42（1）条所述的数据保护认证机制应考虑的要求。

9 欧洲委员会可以采取措施规定认证机制和数据保护印鉴和标识的技术性标准。行动应当根据第 93 条第 2 款的规定进行实施。

第五章. 个人数据向第三国或者国际组织的传输

第 44 条 传输的一般原则

任何正在处理中的个人资料的转让，或在转往第三国或国际组织后拟处理的个人资料的转让，只有在符合本规例其他条文的规定下，才可进行转让，而本章所订的条件，包括将个人资料由第三国或国际组织转往另一第三国或另一国际组织的条件，均须由控制者和处理者遵守。为确保本章所保证的自然人的保护级别不受到损害，本章的所有规定都应执行。

第 45 条 基于充分决定的数据传输

1 对第三方或国际组织进行个人数据的传输，发生在如下情形时，不需要任何的授权：即当欧洲委员会已确定了的要求信息的第三国或其中某一地区或一个或多个特定的地区、或国际组织，有足够级别的保护。

2 当对保护级别的充分性进行评估的时候，欧洲委员会将会特别地考虑以下因素：

a) 法律条文，尊重人权和基本自由，一般性和部门性的相关立法，包括涉及公共安全、国防、国家安全和刑法的，以及公共当局查阅个人数据的相关立法，以及此类立法，数据保护规范、行业法规和安全措施的实施，包括个人数据向其他第三国或国际组织传输的规则，这些规则都应符合该国或该国际组织的相关法规和政策、判例法，以及有效及强制的数据主体权利，并对个人数据被传输的主体进行有效的行政管理和司法补救。

b) 第三国或一个国际组织所属一个或多个独立监督机构的存在和有效运作，或对于某一国际组织为主体的，负责确保和强制遵守数据保护规则，包括适当的执法权，用于在数据主体行使其权利时提供辅助和指导，以及用于与各成员国监管部门进行合作；

c) 第三国或有关国际组织已作出的国际承诺，或法律上具有约束力的

公约或文书所产生的其他义务，以及其参与多边或区域制度，特别是与保护个人资料有关的义务

3 委员会在对保护级别的充足性进行评估之后，可通过实施法案的方式，决定第三国，或其某一地区或某些特定部门，或某一国际组织确保本条第 2 款所指的适当保护水平。执行法案应规定一个定期审查的机制，至少每四年为一个周期，该机制应考虑到第三国或国际组织内的所有相关发展。执行法应具体说明其领土和部门适用情况。并酌情指明本条第 2 款(b)项所指的监督机构或当局。该法案的执行应按照第 93 条第 2 款所述的审查程序被通过。

4 欧洲委员会应持续监控第三国或国际组织可能影响到根据本条第 3 款通过的决定和根据第 95/46/EC 号指令第 25(6)条通过的决定的发展情况。

5 当有可靠信息显示，特别是依据本条第 3 款所述的审查程序，某第三国，其中的某区域或一个或多个特定的部门，或者某国际组织，依据本条第 2 款的含义，不再能够确保足够的保护级别时，在必要的程度上，国会将会依据本条第 3 款，通过实施无追溯效力的行动，来撤销、修订或终止该决定。此类实施行动将会依据第 93 条第 2 款的检验步骤通过并采用。

在合理的必要紧急情况下，欧洲委员会应依据第 93 条第 3 款所述程序，立即采取适用的实施行动。

6 欧洲委员会应与第三国或国际组织进行协商，以期纠正导致据第 5 款所作决定的情况。

7 根据本条第 5 款做出的决定不妨碍根据第 46 至 49 条向第三国、该第三国境内的一个地区、一个或多个特定部门或有关国际组织转让个人资料。

8 委员会应在"欧洲联盟公报"及其网站上公布第三国家、第三国和国际组织中的特定区域和特定部门的名单，以及其充分保护是否得到或者不在得到保证的情况。

9 欧洲委员会根据第 95/46/EC 号法令第 25 条第 6 款所通过的决定将继续有效，直至欧洲委员会根据本条第 3 或第 5 款所通过的决定予以修正、取代或废止。

第 46 条　主体转移的保障措施

1 在缺乏根据第 45 条第 3 款所作决定的情况下，仅当在控制者或处理者

提供了适当的安全措施，以及在可强制执行的数据主体权利和对数据主题的有效法律补救措施时就绪的条件下，一个控制者或处理者可以将个人数据转移到第三个国家或国际组织。

2 第 1 款所述适当的保障措施，可在不需要监督机构任何具体授权的情况下，通过以下方式提供：

a) 政府当局或公共机构之间具有法律约束力的、可执行的工具；

b) 依照第 47 条制定的具有约束力的公司规则；

c) 欧洲委员会根据第 93 条第 2 款所述审查程序通过的标准数据保护条款；

d) 监察机构根据第 93 条第 2 款所述审查程序通过的标准数据保护条款；

e) 根据第 40 条的规定批准的行为准则，以及第三国控制者或处理者的具有约束力的、可执行的，用以采用适当保障措施约定，包括关于数据主体权利的；或

f) 根据第 42 条获得批准的认证机构，以及第三国控制者或处理者的具有约束力的、可执行的，用以采用适当保障措施约定，包括关于数据主体权利的。

3 根据监管主管部门的授权，特别地，参照第 1 款所述的适当保障措施也可通过以下方式提供:

a) 在第三国或国际组织中，控制者或处理者与控制者、处理者或个人数据接受方之间的合同条款；或

b) 被纳入政府当局或公共机构之间行政安排的规定，其中包括可执行的、有效的数据主体权利。

4 对于本条第 3 款所述情况，监察机构应运用第 63 条所述的一致性机制。

5 根据第 95/46/EC 号指令第 26 条第 2 款的规定，由成员国或监督机构发出的授权应继续有效，直至必要时由该监督机构予以修正、取代或废除。欧洲委员会根据第 95/46/EC 号指令第 26 条第 4 款所通过的决定将继续生效，直至必要时被根据本条第 2 款所通过的欧洲委员会决定所修正、取代或废除。

第 47 条　约束性合作法规

1 主管监督机构应根据第 63 条规定的一致性机制，批准具有约束力的公司规则，前提是这些规则满足如下条件：

a) 具有法律约束力，并适用于每一个从事联合经济活动的企业集团或事业集团，且包括其雇员在内；

b) 明确授予数据主体在处理个人数据时的可强制执行的权利；且

c) 满足第 2 款所述的要求。

2 第 1 款所指的具有约束力的公司规则应至少明确规定：

a) 从事联合经济活动的事业集团或企业集团、及其各个成员之间的结构和联系详情；

b) 数据传输或传输集，包括个人数据类别、处理类型及其目的、所涉及的数据对象类型以及对第三国或各国家的确认；

c) 具有法律约束力的性质，包括内部和外部的；

d) 通用数据保护原则的应用，特别是目的限制，数据最小化，存储周期限制，数据质量，设计的和默认的数据保护，处理过程的法律依据，特殊类别个人数据的处理，确保数据安全的措施，向不受具有约束力的公司规则约束的机构转移的要求；

e) 数据主体在处理方面的权利和行使这些权利的方式，包括不受完全基于自动处理的决定约束的权利，包括依照第 22 条进行分析的权利，依照第 79 条向主管监督机构和各成员国主管法院提出申诉的权利，并就违反具有约束力的公司规则而获得补救和酌情获得赔偿；

f) 在成员国领土内建立的控制者和处理者接受非欧盟内的任何有关成员违反有约束力的公司规定的任何责任；控制者或处理者须全部或部分豁免该法律责任，但须证明该成员对造成损害的事件不负责任；

g) 除第 13 条和第 14 条之外，关于有约束力的公司规则的信息，特别是关于本款（d）、（e）和（f）项所指的规定，是如何提供给数据主体的；

h) 根据第 37 条所指定的数据保护官员，或其他任何个人或实体，用于负责对参与联合经济活动的事业或企业集团是否遵从有约束力的公司规定进行监控，以及对培训和投诉处理进行监控；

i) 申诉程序；

j) 从事联合经济活动的事业或企业集团内部，用于确保对有约束力的公司规则的遵守情况进行核查的机制。这种机制应包括数据保护审计和确保校正措施的方法，以保护数据主体的权利。该核查结果应告知(h)项中所指的人或实体，以及负责管控的理事会，该理事会对从事联合经济的活动的事业和企业集团进行管控，并应可供主管监督机构查用；

k) 对规则变动进行记录和报告、并向监督机构报告这些变化的机制；

l) 与监管当局合作的机制，以确保任何企业集团成员或从事联合经济活动的企业集团成员遵守该机制，特别是通过向监督机构提供第(j)项所述措施的核查结果；以及

m) 向主管监督机构就合法要求进行报告的机制，参与联合经济活动的事业或企业集团的成员在第三国作为主体，可能会对具有约束力的公司规则所提供的保障产生重大的不利影响。

n) 对永久或定期访问个人数据的人员进行适当的数据保护培训。

3 欧洲委员会可以具体规定控制者、处理者和监督机构之间信息交换的格式和流程。以便在本条所指的范围内（执行）具有约束力的公司规则，其实施过程应按照第 93 条第 2 款规定的审查程序通过。

第 48 条　未经欧盟授权的传输或者披露

法院或法庭的任何判决以及第三国行政当局要求控制人或处理者转让或披露个人数据的任何决定，只有在以任何方式得到承认或强制执行时，才能基于请求国与欧盟或成员国之间生效的国际协定，如司法协助条约，而不影响根据本章转让的其他理由。

第 49 条　具体情形下的部分违反

1 依照第 45 条第 3 款没有做出适当的决定，或依照第 46 条没有适当的安全措施，包括具有约束力的公司规则，向第三国或国际组织转让个人资料，只应在下列条件之一下进行：

a) 该数据转移由于缺乏适当的决定和适当的保障措施而存在的潜在风险，已通知到数据主体之后，数据主体已明确同意拟议的转移；

b) 转移是数据主体与控制人之间履行合同所必需的，也是应数据主体的要求采取的预合同措施的实施所必需的；

c) 为取得控制权人与另一自然人或法人之间的数据主体利益而订立或履行合同时，该数据转移是必要的；

d) 出于公共利益的重要原因，必须进行数据转移的；

e) 该数据转移对于建立、行使或捍卫法律权利是必要的；

f) 为了保护数据主体或其他人的切身利益，在数据主体的身体或法律上没有能力表示同意时，转让是必要的；

g) 根据欧盟或成员国法律，转移是从一个寄存器开始的，是为了向公众提供信息，一般公众或任何能够证明合法利益的人都可以咨询，但只有在符合特定的欧盟或成员国法律规定的协商条件时才能进行转让。

数据转移无法依据第 45 和 46 条规定，包括约束性企业规则，也没有任何违反本条第 1 分款中提到的特殊情况的，只关注有限数量数据主体的情况下，则只有在转让不再重复的情况下，才可向第三国或国际组织转移，这对于控制者所追求的强制法律权利的目的是必要的，且不得被数据主体的利益或权利和自由所覆盖。控制者对数据传输周边情况进行了评估，并在此基础上提供了关于个人数据保护的适当保障措施。控制人应当将数据转移情况告知监督机构。除提供第 13 条和第 14 条所述的信息之外，控制者还应将转移数据和所追求的强制法律权利告知数据主体。

2 根据第 1 款第 1 分款的第(g)项进行的数据转移，不应涉及寄存器内所载的全部个人数据或个人数据的全部类别。如寄存器拟由具有合法权益的人查阅，则只有在这些人提出请求或他们是接收人的情况下，才应进行转让。

3 第 1 款和第 2 款的第 1 分款的第(a)、(b)和(c)项不应适用于政府当局行使其公共权力所进行的活动。

4 第 1 款第一分款第(d)项所述的公众利益，应在欧盟法律受控制者管辖的成员国的法律中得到承认。

5 在没有适当决定的情况下，欧盟或成员国法律可能出于公共利益的重要原因，明确规定要向某第三国或某国际组织转移的个人数据的具体类别。成员国应将这些规定通知欧洲委员会。

6 控制者或处理应以书面形式，将评估报告和本条款第 30 条第 1 款第 2 分款所述的适当保障措施记录在案。

第 50 条　关于个人数据的国际合作

关于第三国和国际组织，欧洲委员会和监督机构应采取适当步骤以:

a) 制订国际合作机制，以促进保护个人数据法规的有效执行；

b) 在执行保护个人数据法规方面提供国际互助，包括通过通知、投诉咨询、调查援助和信息交换，以适当的保障措施保护个人数据和其他基本权利和自由；

c) 使有关利益相关方参与到讨论和活动中，以促进保护个人数据法规执行方面的国际合作；

d) 促进个人数据保护法例和实务的交流以及文件编制工作，包括与第三国的管辖权冲突问题。

第六章. 独立的监督机构

第一节. 独立地位

第 51 条　监督机构

1 各成员国应提供一个或多个独立的政府公共机构，用以负责监控本法案的应用，目的在于保护与处理程序相关自然人的基本权利和自由，并促进欧盟内个人数据的自由流动。

2 各监督机构应致力于本法案在整个欧盟中的贯彻应用。为此，各监督机构应按照第 VII 章的规定，在相互之间和与欧洲委员会之间进行展开合作。

3 多个监督机构在同一成员国建立时，成员国应指定哪个监督机构能够在理事会中代表所有这些监督机构，并应当制定相应机制，以确保其他机构依从第 63 条所指一致性机制中的规定。

4 各成员国应在 2018 年 5 月 25 日之前，将其根据本章所通过的法律规定通知到欧洲委员会，并在不延误的情况下通知委员会有权对随后对其产生影响的任何修正。

第 52 条　独立性

1 各监督机构在执行任务时，应完全独立行动，并依照本法案行使职权。

2 各监督机构的某个或某些成员在按照本法案的规定执行任务和行使职

权时，须不受直接或间接的外来影响，且不得寻求或接受任何人的指示。

3 各监督机构的成员应避免任何与其职责不符的行为，在其任期内不得从事任何不相容的职业，不论是否有收益。

4 各成员国应确保向每个监督机构提供有效执行其任务和行使其权力所需的人力、技术和财政资源以及经营场所和基础设施，包括在理事会中相互协助、合作和参与的情况下进行工作。

5 每一成员国应确保每一个监督机构的选择并拥有自己的工作人员，其工作人员应受有关监督机构成员的排他性指导。

6 每个成员国应确保每个监督机构受不影响其独立性的财务控制，并且确保它有独立的、可能是整个政府或者国家预算一部分的公共年度预算。

第 53 条　监督机构成员的一般条件

1 成员国应通过以下透明程序任命其监督机构的每一名成员：

a) 他们的议会；

b) 他们的政府；

c) 国家元首；或

d) 根据成员国法律委任的独立机构。

2 每个成员应具备满足其履行其职责并行使其权力需求的资质、经验和技能，特别是在个人数据保护方面。

3 在任期届满、辞职或强制退休的情况下，成员的责任应依照有关成员国法律终止。

4 某一成员只有在严重行为不当或不再满足履行职责所要求的条件时，才可被开除。

第 54 条　关于监督机构建制的规定

1 各成员国应根据法律规定满足下列各项:

a) 设立各监督机构；

b) 被委任为监督机构成员所需的任职资格及资格条件；

c) 任命各监督机构成员的规则和程序；

d) 每个监督机构成员的任期不得少于四年，2016 年 5 月 24 日的第一

次委任除外，其中有可能发生任期为时较短的情况，此时有必要通过交错任命程序来保护监管部门的独立性；

e) 监督机构的成员是否有资格连任，如有资格，任期是多少；

f) 每一个监督机构的成员和工作人员的义务，禁止在任期内和任期结束后的行动、职业和福利方面的规定以及停止雇用的规则。。

2 根据欧盟或成员国法律，各监督机构的成员和工作人员在任期内和任期后，对于在执行任务或行使权力过程中获悉的任何机密信息，均应承担保密义务。在任期内，这一专业保密义务特别适用于自然人举报违反本法规的行为。

第二节. 权限、任务和职权

第 55 条 权限

1 每个监督机构应有权在其成员国领土上执行根据本法规赋予它的任务和行使其所获得的权力。

2 如果由公共当局或私营机构根据第 6 条第(1)款(C)或(E)项进行处理，则有关成员国的监督机关应具有管辖权，在这种情况下，第 56 条不适用。

3 监督管理部门无权监督法院处理其司法能力内的工作。

第 56 条 主监督机构的权限

1 不违背第 55 条的情况下，主监督机构的监管部门、控制者或处理者的单一机构有权根据第六十条规定，担任该控制者或处理者进行的跨界处理的主管监督机构。

2 当违反第一款时，如果所涉事项仅涉及其成员国的机构或仅影响其成员国的数据主体，每一监督机构均有权处理向其提出的申诉或可能违反本法规的行为。

3 涉及本条第 2 款所述的情况时，监督机构应第一时间通知主监督机构。在接到通知后的三周内，主监督机构应根据第 60 条规定的程序决定是否处理该案件，同时考虑是否监督机关通知了建立在其会员国中的控制者或处理者。

4 若主监督机构决定受理该案件，则应实行第 60 条所规定的程序。通知主监督机构的监督机构，可向主监督机构提交一份决定草案。主监督机

构在依据第 60 条第 3 款拟订决定草案时，应最大限度地参考该草案。

5 若主监督机构决定不受理该案件，通知主监督机构的监督机构应根据第 61 条和第 62 条的规定处理该案件。

6 主监督机构是跨境处理过程的控制者或处理者的唯一对话者。

第 57 条　任务

1 在不损害本法规规定的其他任务的原则下，各监督机构应在其管辖区域内:

a) 监管和推进本法规的执行；

b) 提高公众对与处理有关的风险、规则、保障措施和权利的认识和理解，加强面向儿童的活动；

c) 根据会员国法律，为国家议会、政府和其他机构和团体，就有关保护自然人的权利和自由的立法和行政措施所提出建议；

d) 提高管理器和处理者对本法案所规定义务的认识；

e) 根据要求，向任何本规定下有关行使其权利的数据主体提供资料，并酌情，同其他成员国的监督机构就此进行合作；

f) 依照第 80 条处理数据主体、团体、组织或协会提出的申诉，并在适当范围内调查投诉的主题，并在合理期间内将调查的进展和结果通知投诉人，特别是在需要进一步调查或与其他监督机构合作的情况下；

g) 与其他监督机构合作，包括信息共享和提供相互协助，以确保本规定的适用和执行的一致性；

h) 就本规定的应用进行调查，包括根据从另一监督机构或其他公共机构收到的资料；

i) 监测有关的发展，只要它们对保护个人资料有影响，特别在信息通信技术和商业行为方面；

j) 采用第 28 条第 8 款和第 46 条第 2 款所指的标准合同条款；

k) 根据第 35 条第 4 款，建立和保持一份与数据保护影响评估要求有关的清单；

l) 就第 36 条第 2 款所述的处理行动给出意见；

m) 鼓励根据第 40 条第 1 款拟订行为准则，并根据第 40 条第 5 款，提出意见并核批提供充分保障的行为准则；

n) 鼓励根据第 42 条第 1 款所述建立的数据保护认证机制和数据保护印鉴和标记，并根据第 42 条第 5 款所述批准通过认证标准；

o) 在适当的情况下，定期审查根据第 42 条第(7)款颁发的证书；

p) 起草并公布第 41 条规定的行为守则监测机构和第 43 条规定的认证机构的认证标准；

q) 根据第 41 条规定的用于监控行为准则的机构的评审标准和根据第 43 条规定的认证机构的评审标准的管理实施；

r) 授权第 46 条第 3 款所述的合同条款和规定；

s) 根据第 47 条批准有约束力的公司规则；

t) 协助理事会的活动事宜；

u) 保存违反本法规和根据第 58 条第(2)款采取措施的内部记录；和

v) 完成与个人数据保护有关的任何其他任务。

2 每一监督机构应采取诸如投诉提交表格等措施，协助便利提交第 1 款 (f)项所指的投诉，该表格也可以用电子方式提交，但也不排除其他通讯方式。

3 各监督机构的任务执行应免费向数据主体提供，并在必要时向数据保护官员提供。

4 如果请求显然无根据的或过多的，特别是重复的请求，监督机构可以根据行政费用规定进行合理收费，或拒绝此请求。监督机构应承担举证责任，证明请求明显无根据或过多。

第 58 条　职权

1 每一监督机构都应拥有以下所有调查权力:

a) 责令控制者和处理者，以及在适用的情况下，控制者或处理者的代表，提供其执行任务所需的任何信息；

b) 以数据保护审计的形式进行调查；

c) 对据第 42 条第 7 款所发的证书进行审查；

d) 将涉嫌违反本法规的人通知控制者或处理者；

e) 从控制者和处理者中获取所有个人数据和执行其任务所需的所有必要信息；

f) 根据欧盟或成员国的程序法规，获得对控制者和处理者的任何经营场所，包括对任何数据处理设备和手段的访问权。

2 各监督机构应具备以下所有校正权利:

a) 向处理业务过程中有可能违反本法规的控制者或处理者发出警告；

b) 向处理业务过程中已违反本法规的控制者或处理者发出谴责；

c) 命令控制者或处理者遵守数据主体根据本规定行使其权利的要求；

d) 适当情况下，在特定的时间以特定的方式命令控制者或处理者使处理操作符合本规定；

e) 命令控制者将个人数据泄露情况传达给该数据主体；

f) 对处理过程施加临时或明确的限制，包括禁止令；

g) 根据第 16 条、第 17 条和第 18 条，命令更正或删除个人资料或限制其处理，并向根据第十七条第二款和第十九条向其披露个人资料的收件人通知此类行动；

h) 撤销认证或命令认证机构撤回根据第 42 条和第 43 条发出的认证，或要求认证机构在认证要求不满足或不再满足的情况下不颁发证书；

i) 根据第八十三条的规定，除本款所述措施外，根据每一案件的具体情况，处以行政罚款；

j) 下令暂停流向第三国或国际组织的接受者的数据流。

3 各监督机构应有以下所有授权和咨询权力:

a) 按照第三十六条所述的事先协商程序，向控制者提供意见。；

b) 主动或应请求就任何与保护个人数据有关的问题向国民议会、成员国政府或根据会员国法律向其他机构和团体以及公众发表意见；

c) 如果成员国的法律要求事先批准，授权第 36 条第(5)款所述的处理；

d) 根据第 40 条第(5)款发表意见并核准行为守则草案；

e) 依照第 43 条授权认证机构；

f) 根据第四十二条第(五)款颁发证书和批准认证标准；；

g) 通过第 28 条第(8)款和第 46 条第(2)款(D)项所述的标准数据保护条款；；

h) 授权第四十六条第(三)款(A)项所指的合同条款；

i) 授权第四十六条第(三)款第(二)项所述的行政安排；

j) 根据第 47 条批准具有约束力的公司规则。

4 根据本条赋予监督机构权力的行使，应遵守"宪章"规定的适当保障措施，包括有效的司法补救办法和正当程序，这些措施应在欧盟和成员国法律中规定。

5 每一成员国应依法规定，其监督机构有权提请司法当局注意违反本法规的情况，并酌情启动或以其他方式进行法律程序，以执行本法规的规定。

6 每一成员国可根据法律规定，其监督机构应比第 1、2 和 3 款所述的机构拥有更多的权力。行使这些权力不得损害第 VII 章的有效运行。

第 59 条　活动报告

每个监督机构应就其活动起草年度报告，其中可包括已通知的侵权类型和根据第五十八条第(2)款采取的措施类型。这些报告应转交国家议会、政府和会员国法律指定的其他主管部门。它们应向公众、委员会和董事会提供。

第七章. 合作与协调

第一节. 合作

第 60 条　主监督机构与其他相关监督机构的配合

1 主监督机构当按照本条的规定与其他相关的监督机构合作，努力达成共识。主监督机构和监督机构应当互相交换有关资料。

2 主监督机构可随时请求其他有关监督机构根据第六十一条提供互助，并可根据第六十二条开展联合行动，特别是为进行调查或监测与另一成员国设立的控制器或处理器有关的措施的执行情况。

3 领导监督机构应当及时向有关主管机关通报有关情况，并立即将决定草案提交其他有关监督机构征求意见，并适当考虑其意见。

4 如果其他有关监督机构在根据本条第 3 款，与之协商后四周内对决定草案表示了相关和有理由的反对，则主监督机构如不遵循相关的和理由充分的反对意见，或认为该反对不相关或无理由，应将该事项提交给第六十三条所述的一致性机制。

5 主监察机关对提出的有关理由提出异议的，应当向其他有关监督机关提出修改后的决定草案，征求其意见。经修订的决定草案应在两周内遵守第 4 款所述程序。。

6 其他有关监督机关在第四款和第五款所述期间内未对牵头监督机构提交的决定草案提出异议的，应当视为同意该决定草案，并受其约束。

7 主管监督机关应当根据具体情况，将决定通知主要机构或单一机构控制者或处理者，并将有关决定通知其他有关监督机构和欧盟，包括有关事实和理由的摘要。向其提出申诉的监督机构应将决定通知申诉人。

8 如投诉被驳回或被拒绝，则向其提出申诉的监督当局须藉减损第 7 段规定而采纳该决定，并将该决定通知投诉人，并须将该决定通知控制者。

9 主监督机构和有关监督机构同意驳回或拒绝部分投诉，并就该投诉的其他部分采取行动时，应就该事项的每一个部分分别做出决定。主监督机关应就与控制者有关的行动部分做出决定，应通知其在其成员国领土上的主要机构或单一机构，并应将此事通知申诉人，而投诉人的监察当局须就有关驳回或拒绝该投诉的部分做出决定，并须将该决定通知该投诉人，并须将此事通知控制者或处理者。

10 在接到主管监督机构根据第 7 和第 9 款做出决定的通知后，控制者或处理者应采取必要措施，确保在欧盟范围内的所有机构遵守关于处理活动的决定。控制者或处理者应当把为执行决定而采取的措施通知给主监督机关，由主监督机关通知其他有关监督机构。

第 61 条　相互协助

1 监管部门应相互提供相关信息和相互协助，以一致的方式实施和应用本法规，并制定有效合作措施。相互援助应特别包括信息请求和监管措施，例如事先授权和协商、检查和调查的请求。

2 各监督机构应采取一切必要的适当措施，在收到请求后一个月内，不得无故拖延对另一监督机构的请求的答复。这类措施包括转交进行的有关调查的资料。

3 请求援助应包含所有必要的信息，包括请求的目的和理由。所交换的资料应仅用于所要求的目的。

4 被请求的监督机构不应拒绝遵从该请求，除非:

a) 它无权处理该请求的主体相关事宜或要求其执行的措施；或

b) 遵从该要求会违反本法规、欧盟法律或接受请求的监督机构所属成员国法律。

5 被请求的监督机构应将结果或(视情况而定)为回应请求而采取的措施的进展情况通知提出请求的监督当局。被请求的监督机构应说明拒绝遵守第 4 款规定的请求的理由。

6 被请求的监督机构通常应采用标准化格式，以电子方式提供其他监督机构所要求的信息。

7 被请求的监督机构不应对其根据互助请求采取的任何行动收取费用。监督机关可以就在特殊情况下提供互助所引起的具体支出相互赔偿的规则达成协议。

8 监督机关在收到另一监督机关的请求后一个月内未提供本条第五款所述信息的，请求监督机构可根据第五十五条第一款在其成员国领土上采取临时措施。在这种情况下，根据第 66 条第(1)款采取行动的迫切需要应假设满足，并要求欧盟根据第 66 条第(2)款做出具有约束力的紧急决定。

9 委员会可通过实施法案，具体说明本条所述的相互协助的格式和程序，以及监督当局之间和监督机构与理事会之间以电子方式交流信息的安排，特别是本条第 6 款所述的标准化格式。第九十三条第二款规定的审查程序，应当采取实施措施。

第 62 条　监督机构联合行动

1 监督当局应酌情开展联合行动，包括联合调查和联合执法措施，由其他成员国监督机构的成员或工作人员参与。

2 控制者或处理者在几个成员国设有机构，或在一个以上的成员国中有相当数量的数据主体可能会受到处理行动的严重影响，则每个会员国的监督机构应有权参加联合行动。根据第五十六条第(一)款或第(四)款主监督机构应邀请每一成员国的监督机构参加联合行动，并应立即对监督机构

提出的参加联合行动请求做出回应。

3 监督机构可以根据成员国法律和第二监督机构的授权，授予权力，包括授权第二监督机构的成员或参与联合行动的工作人员，或在主监督机构法律允许的范围内，允许将监管部门的成员或职员按照第二监督机构所在成员国法律，行使调查权。只有在东道国监督机构的成员或工作人员在场的情况下，该调查权才能得以行使。第二监督机构的成员或工作人员应遵守东道国监督机构的成员国法律。

4 依照本条第 1 款，第二监督机构的工作人员在另一成员国工作，主监督机构所在成员国应根据其所在领土上的会员国的法律，对其业务期间所造成的任何损害承担责任，包括赔偿责任。

5 在其领土内造成损害的会员国应按照适用于本国工作人员造成的损害的条件赔偿这种损害。第二监督机构的成员国，其工作人员在另一会员国领土内对任何人造成损害的，应全额赔偿另一会员国支付给有权代表该另一会员国人的任何款项。

6 在不妨碍第三方行使除第五款的权利下，每一成员国应避免第一段中提到的情况，即另一成员国提出就第 4 款所述损害的赔偿要求。

7 在联合行动筹备中，一个月内，监管部门不遵守本文第 2 款的第二句所规定义务的情况下，其他监督机构可依照第 55 条在其成员国的区域内采取临时措施。在这种情况下，应假定满足采取第 66 条第 1 款所述行动的迫切需求，并根据第 66 条第 2 款请求意见或具有约束力的紧急决定。

第二节. 一致性

第 63 条 一致性机制

为了促进本法案在整个欧盟内的一致应用，监督机构之间应相互合作，并在合适的时候与欧洲委员会通过本节提到的一致性机制相互配合合作。

第 64 条 理事会的处理意见

1 理事会应在主管当局采取下列任何措施时发表意见。为此，主管监督机构应将决定草案传达给理事会，当：

a) 旨在依照第 35 条第 4 款的规定，通过一份符合数据保护影响评估要求的处理操作清单；

b) 考虑第 40 条第 7 款的规定，行为准则草案、修正案或其延伸是否遵守本法规；

c) 根据第 41 条第 3 款或根据第 43 条第 3 款的相关规定，旨在核准一个机构的认证标准；

d) 旨在确定第 46 条第 2 款 (d) 项和第 28 条第 8 款所指的标准数据保护条款；

e) 旨在授权第 46 条第 3 款(a)项所指的合同条款；或

f) 旨在批准第 47 条的含义内的具有约束力的公司规则。

2 任何监督机构，理事会或欧洲委员会的主席均可要求理事会对任何在不少于一个成员国中的普通应用或产生的效应进行检验，以期征求意见，特别是在监督主管部门未遵守第 61 条互助义务或第 62 条联合行动义务的情况下。

3 在第 1 和第 2 款所述的案件中，理事会应就提交给它的事项发表意见，但须尚未就同一事项发表意见。该意见应在八周内得到理事会过成员过半数通过。考虑到主题的复杂性，这一时期可能会额外延长六周。关于按照第 5 款的规定分发给理事会成员的基于第 1 款的决定草案，未在主席指定的合理期限内提出异议的，应视为同意该决定草案。

4 监督机构和欧洲委员应在无不当拖延的情况下，以标准化格式，电子方式向理事会通报任何有关信息，包括事实摘要、决定草案、制定此类措施的理由以及其他有关监督机构的意见。

5 理事会主席应以电子方式进行如下通告，不得无故拖延：

a) 理事会成员和委员会成员以标准化格式向其通报的任何相关资料。理事会秘书处应在必要时提供有关资料的译文；以及

b) 视情况而定，向在第 1 和第 2 款中所述的相关监督机构和欧洲委员会通告意见，并将其公诸于众。

6 主管监督机构不得在第 3 款所述期间通过第 1 款所述的决定草案。

7 本条第一款所述监督机构应最大限度地考虑理事会的意见，并应在收到意见后两周内，以电子方式向理事会主席通报是否维持或修正其决定草案，如果有任何修订，将采用标准化格式修订决定草案。

8 在本条第 7 段所述期间内，如果监督机构打算全部或部分不遵照理事会

意见的消息，需提供相关理由，并遵照第 65 条第 1 款规定。

第 65 条　理事会争端解决

1　为确保本法规在个别案例中的正确和一致的应用，理事会应在下列情况下做出有约束力的决定:

a) 在第 60 条第 4 款所述的案件中，有关监督机构已对主监督机构的决定草案提出了相关且合理的反对意见，或主监督机构因其相关性和合理性不足而拒绝了该反对意见。具有约束力的决定应考虑相关且合理的反对意见所属主体所涉及的所有事项，特别是是否有违反本法规的情况；

b) 对于哪些监管当局能够胜任主要机构，存在着相互矛盾的观点；

c) 主管监督机关在第六十四条第一款所指案件中不征求董事会意见或者不遵循委员会根据第六十四条发表的意见的，在这种情况下，任何有关的监督机构或委员会可将此事通知理事会。

2　第 1 款所述决定应在提交主题事项之日起一个月内以理事会成员三分之二多数通过。根据主题的复杂性，该期限可另外延长一个月。第 1 款提到的决定，应该向主监察机关和所有相关的且被约束的监察机关说明原因并做出解释。

3　理事会在第 2 款所指期间内不能做出决定的，应当在第 2 款所述第二个月的有效期满之后的两周内做出决定，该决定应得到理事会成员过半数通过。理事会成员意见分歧，由其主席表决通过。

4　在第 2 和 3 款所述期间，有关监督机构不得就第 1 款向欧洲委员会提交的主题事项做出决定。

5　理事会主席应无不当拖延地将第 1 款所述的决定通告有关监督机构，也应通知欧洲委员会。该决定应在监督机构被告知第 6 款所述最终决定后，立即在理事会网站上公布。

6　主监督机构或向其提出申诉的监督机构，应根据本条第 1 款所述决定，做出最后决定，不得无故拖延，最迟应在董事会通知其决定后一个月内做出最后决定。主监督机构或向其提出申诉的监督机构，应将其最后决定分别通知控制者、处理者以及数据主体，有关监督机构的最后决定应根据 60(7), (8) 和(9)予以通过。最终决定应参照本条第一段所述决定，应指明该款所述决定将按照本条第 5 款在理事会网站上公布。最后决定

应附于本条第 1 款所述的决定。

第 66 条　紧急程序

1　在特殊情况下，如果有关监督机构认为迫切需要采取行动，以保护数据主体的权利和自由，它可能通过限制第 63、64 和 65 条所述一致性机制，或第 60 条所述程序，立即采取临时措施，以便在其本国领土上产生有效期不得超过三个月的法律效力。监督机构应及时将这些措施和采取这些措施的理由与其他有关监督机构、理事会和欧洲委员会进行沟通。

2　如果监督机构已根据第 1 款采取措施，并认为迫切需要采取最后措施，可以向欧洲委员会请求紧急意见或有约束力的紧急决定，并给出提请该意见或决定的理由。

3　在保护数据主体的权利和自由时，如果主管监督当局在迫切需要采取合适措施时却没有采取措施，任何监管机关均可视情况向理事会请求紧急意见或具有约束力的紧急决定，并说明要求提供这种意见或决定的理由，包括迫切需要采取行动的理由。

4　根据第 64 条第 3 款和第 65 条第 2 款的限制，本条第 2 款和第 3 款所述的紧急意见或有约束力的紧急决定应在两周内获得理事会成员半数通过。

第 67 条　情报交换

欧洲委员会可采取一般范围的执行行动，以便具体规定监督当局之间以及监督当局与理事会之间以电子方式交流信息，特别是第 64 条所述的标准化格式。

这些执行行为应当按照第 93 条第 2 款所述的审查程序通过。

第三节.　欧盟数据保护理事会

第 68 条　欧盟数据保护理事会

1　特此设立欧洲数据保护理事会("理事会")，作为欧盟的一个机构，具有法人资格。

2　理事会应由其主席代表。

3　理事会由各成员国的一个监督机构的负责人和 EDPS[1]或其各自的代表组

[1] European Data Protection Supervisor，欧洲数据保护主管。

成。

4 在成员国中，有一个以上的监督机构负责监督本法案各项规定的适用情况，应按照该成员国的法律任命一名联合代表。

5 委员会有权在没有投票权的情况下参加理事会的活动和会议。委员会应指定一名代表。理事会主席应向委员会通报理事会的活动。

6 在第 65 条所述的案件中，EDPS 只对涉及适用于欧盟各机构、机关、办事处和机构的原则和规则的决定拥有表决权，这些决定实质上与本法规的原则和规则相对应。

第 69 条　独立性

1 理事会在根据第七十条和第七十一条执行任务或行使权力时，应独立行事。

2 在不违反第七十条第(一)项(B)项和第七十条第(二)款所述委员会的要求的情况下，理事会应在执行其任务或行使其权力时，不得寻求或接受任何人的指示。

第 70 条　理事会的任务

1 理事会应确保本法规的一致适用。为达到此目的，理事会应主动或在相关情况下应委员会的请求，特别是:

a) 在不妨碍国家监督机构的任务的情况下，监督和确保在第 64 条和第 65 条规定的情况下正确适用本法规；

b) 就任何与保护本欧盟个人资料有关的问题，包括就本规例的任何拟议修订，向委员会提供意见；

c) 就控制者、加工者和监督当局之间交流信息的格式和程序向委员会提供咨询意见，以制定具有约束力的公司规则；

d) 发布从第 17 条第 2 款所述的公开通讯服务中删除个人数据的连接、复制或副本的指导方针、建议和最佳实践方案；

e) 自发地，或根据欧洲委员会成员的要求或欧洲委员会的要求，审查涉及本法规应用的任何问题，并提出指导方针、建议和最佳实施方案，以鼓励本法规的一致应用；

f) 按照本款的 (e) 项发布指导方针、建议和最佳实施方案，进一步根

据第 22 条第(2)款的概要分析制定决策的标准和条件；

g) 按照本款(e)项提出指导方针，建议和最佳实施方案，建议和最佳做法，以确定第 33 条第(1)款和第(2)款所指的不正当延迟，并确定在何种特定情况下需要控制者或处理者通知个人数据被泄露；

h) 根据本款的第(e)点项，就个人数据泄露可能致使第 34 条第 1 款所指自然人的权利和自由面临高风险的情况，提出指导方针、建议和最佳实施方案。

i) 根据本款的第(e)项，提出指导方针、建议和最佳实施方案，用于基于分别由控制者和处理者遵守的有约束力的企业规定、以及进一步确保第 47 条相关数据主体的数据保护，来进一步明确个人数据传输的标准和要求；

j) 根据本款的第(e)项，提出指导方针、建议和最佳实施方案，以达到进一步说明第 49 条第 1 款规定的个人数据转移的标准和要求；

k) 拟订监督机构关于第 58 条第 1、2 和 3 款所述措施应用相关的指导方针，以及依照第 83 条设立行政罚款的指导方针；

l) 审查项(e)和(f)所述的指导方针、建议和最佳实施方案的实际应用；

m) 根据本款的要点，提出指导方针、建议和最佳实施方案，用于建立的自然人对第 54 条第 2 款所述违反本法的情况进行报告的通用程序；

n) 鼓励编制第 40 条所述行为准则和建立第 42 条所述数据保护认证机制和数据保护印鉴和标记；

o) 按照第 43 条的规定进行认证机构的认定及其定期审查，根据第 43 条第(6)款对经认证的机构和根据第 42 条第(7)款在第三国设立的经认证的控制者或处理者进行公开登记；

p) 明确第 43 条第 3 款所述的要求，以便对第 42 条所述认证机构进行认定；

q) 向欧洲委员会提供对于第 43 条第 8 款所述认证要求的意见；

r) 向欧洲委员会提供对于第 12 条第 7 款所述图标的意见；

s) 为欧洲委员会提供对于第三国或国际组织的防护级别充足性评估的意见，包括对第三国，其中某个地区或一个或多个指定部门，或国际组织是否能继续保证适当保护级别的评估。为此，欧洲委员会应

向理事会提供所有必要文件，包括与第三国政府关于第三国、某区域或指定部门、或与国际组织的通信。

t) 根据第 64 条第(1)款所指的一致性机制就监督机构的决定草案，根据第 64 条第(2)款提交的事项发表意见，并根据第 65 条提出具有约束力的决定，包括第 66 条所述的情况；

u) 促进监督机构之间的合作、有效的双边和多边信息交流以及最佳实施方案；

v) 推动通用培训项目，促进监督机构之间，以及适当情况下与第三国或国际组织的监督机构之间的人员交流；

w))促进与世界各地的数据保护监督机构交流关于数据保护立法和做法的知识和文件；

x) 就按照第 40 条第 9 款拟订的欧盟级别的行为准则发表意见；以及

y) 维持一份公众可查阅的决议电子登记册，记录监督当局和法院就统一机制处理的问题做出的决定。

2 委员会如要求理事会提供咨询意见，可考虑到此事的紧迫性，说明时限。

3 欧洲委员会应将其意见、指导方针、建议和最佳实施方案向欧洲委员会和第 93 条所指的组委会提出，并将其公开。

4 理事会应酌情与有关各方协商，并给予他们在合理期限内发表评论的机会。理事会应在不违反第 76 条的情况下，将协商程序的结果公开。

第 71 条 报告

1 理事会应起草一份年度报告，说明在欧盟以及相关的第三国和国际组织处理过程中保护自然人的情况。报告应公开，并转交欧洲议会、理事会和委员会。

2 年度报告应包括对第 70 条第 1 款(1)项所指指导方针、建议和最佳实践的实际应用情况的审查，以及第 65 条所述的具有约束力的决定的审查。

第 72 条 程序

1 除非本法案另有规定，否则理事会的决定应由其成员的简单多数决定。

2 理事会应由其成员三分之二多数来通过自己的议事程序，并组织自己的业务安排。

第 73 条　主席

1　欧洲委员会应以简单多数从其成员中选出一名主席和两名副主席。

2　主席和副主席的任期为五年，可连任一次。

第 74 条　主席的职责

1　主席应承担如下任务:

a)　召开理事会会议并筹备其议程；

b)　将理事会根据第 65 条所通过的决定通知主监督机构和有关监督机构；

c)　确保理事会任务的及时执行, 特别是与第 63 条所述的一致性机制有关的任务。

2　欧洲委员会应在其议事程序规则中规定主席和副主席之间的任务分配。

第 75 条　秘书

1　理事会设秘书处，由 EDPS 提供。

2　秘书处应完全按照理事会主席的指示履行其职务。

3　EDPS 的工作人员参与执行理事会根据本法规所指派的任务，应与其执行 EDPS 所指派的任务进行分开报告。

4　在适当情况下，委员会和 EDPS 应制定并公布一份执行本条的谅解备忘录，确定其合作条件，以及使其适用于参与理事会根据本法规所指派任务的 EDPS 职员。

5　秘书处应向理事会提供分析、行政和后勤支持。

6　秘书处应特别负责:

a)　理事会的日常业务；

b)　理事会成员、其主席及欧洲委员会之间的交流；

c)　与其他机构和公众进行交流；

d)　利用电子手段进行内部和外部通讯；

e)　有关资料的翻译；

f)　理事会会议的筹备和后续工作；

g) 编制、起草和意见发表、监督机构与欧洲委员会通过的其他案文之间的争端解决机制的决议。

第 76 条　机密性

1 如理事会认为有必要，理事会的讨论应按照其议事规则的规定保密。

2 查阅提交给理事会成员、专家和第三方代表的文件时，应遵守欧洲议会和理事会第 1049/2001 号法规(1)。

第八章. 补救措施，责任以及处罚

第 77 条　向监督机构提出控诉的权利

1 不影响其他任何行政或司法救济的情况下，如果数据主体认为处理与其有关的个人资料违反了本法规，每个数据主体都有权对监督机构提出投诉，尤其是向在其惯常居所、工作地或涉嫌侵权的地点所在的成员国的监督机构。

2 向其提出申诉的监督机构应向申诉人通报申诉的进展和结果，包括根据第 78 条获得司法补救的可能性。

第 78 条　针对监督机构进行司法救济的权利

1 在不损害任何其他行政或非司法补救的情况下，对于监督机构所与其相关的具有法律约束力的决定，每一个自然人或法人都有权获得有效的司法救济。

2 不影响任何其他行政或非司法补救补救的情况下，如果根据第五十五条和第五十六条主管的监督当局没有在三个月内处理申诉，或未在三个月内向数据主体通报根据第七十七条提出的申诉的进展或结果，每个数据主体有权获得有效的司法救济。

3 对监督机构的诉讼，应当向设立监督机构的成员国法院提起。

4 此前监督机构已有在一致性机制方面的意见或决定的，在对监督机构的决定提起诉讼时，监督机构应向法院提供这些意见或决定。

第 79 条　针对数据控制者及处理者的有效的司法救济权利

1 在不影响任何现有的行政或非司法补救办法的情况下，包括依照本法第

77 条向监督机构提起诉讼的权利，每一数据主体如认为其根据本法规享有的权利因以不符合本法规的规定处理其个人资料而受到侵犯的，则应有权获得有效的司法补救。

2 对控制者或处理者的诉讼应在控制者或处理者设有机构的成员国法院提起。此外，该诉讼可提交给数据主体惯常住所所在成员国的法院，除非控制者或处理者是成员国行使其公共权力的公共当局。

第 80 条　数据主体的代理

1 数据主体有权委托非营利机构、组织或协会，该机构、组织或协会按照成员国相应的法律组成，具有符合公共利益的法定目标，并积极参与保护数据主体在保护其个人资料方面的权利和自由，能代表其在个人数据保护方面提出投诉。可代表数据主题使第 77、78 和 79 条所述的权利，并在成员国法律规定的情况下，代表数据主题行使第 82 条所述的获得赔偿的权利

2 独立于数据主体的授权，按照本条第 1 款，该成员国内的任何的机构、组织或协会，在该成员国内都有权向依照第 77 条认定的监督机构提出投诉；如果它认为本法规下的数据主体权利在处理结果中已被侵犯，有权行使第 78 和 79 条所赋予的权利。

第 81 条　中止诉讼

1 某成员国的主管法院获得在另一成员国法庭待定的诉讼信息，该信息与同一控制者或处理者的处理主体事务相同，这种情况下，前者应联系后者法院对该诉讼的是否存在进行确认。

2 与同一控制者或处理者的处理主体事务相同的，正在另一成员国法院待定的诉讼，除了最初接受该案的法院外，其他任何主管法院都可中止该诉讼。

3 如果最初接受该案的法院对所采取的行动具有司法权，且其法律允许合并，对于初审待定的诉讼，基于当事任何一方的申请，除了最初接受该案的法院外，任何法院都可以拒绝行使司法权。

第 82 条　赔偿权及责任

1 任何因违反本法规而遭受物质或非物质损害的人员，均有权自控制者或处理者中就所遭受的损害获取损害赔偿。

2 任何参与处理的控制者都应对违反本法规的处理所造成的损害负责。处理者只有在没有履行本规例特别针对处理者的义务，或在控制者的合法指示之外或相反的情况下，才须对处理所造成的损害负法律责任。

3 如果证明其不该以任何方式对造成损害的事件负责，依据第 2 款，控制者或处理者应免除责任。

4 一个以上控制者或处理者，或两者同时，参与相同处理的情况，以及依据在第 2 和 3 款，他们对处理过程所造成的任何损害负责的情况，每个控制者或处理者应当承担全部损失，以确保数据主体获得有效的赔偿。

5 控制者或处理者依照第 4 款支付了因损害所造成的全部赔偿的，则该控制者或处理者有权按照第 2 款所列的条件，向参与同一处理的其他控制者或处理者追讨与其部分损害责任相应的补偿部分。。

6 法院行使职权以获取赔偿的诉讼程序，应提交第 79 条第 2 款所指成员国法律规定的法院。

第 83 条　征收行政罚款的一般情形

1 每个监督机构应确保根据本条对第 4、5 和 6 款所述违反本法规的行为处以行政罚款，在每一个案中均应有效、相称和具有劝阻性。

2 除第 58(2)条第(a)至(h)及(j)点所提述的措施外，行政罚款须视个别个案的情况而定，在决定是否对每个个案处以行政罚款和决定行政罚款数额时，应考虑下列事项：

a) 侵权行为的性质、严重程度和持续时间，同时考虑相关处理的性质、范围或目的，以及受影响的数据主体的数量及其遭受的损害程度；

b) 违规的故意或过失性质；

c) 控制者或处理者采取的任何措施，旨在减轻数据主体所受损害的；

d) 考虑由第 25 和 32 条所实施的技术和组织措施的情况下，控制者或处理者所承担责任的程度；

e) 控制者或处理者之前发生的任何相关违规行为；

f) 与监督机关的合作程度，以补救侵权行为，减轻侵权行为可能产生的不利影响；

g) 受侵权影响的个人资料类别；

h) 对监督机构获知侵权的方式，特别是该控制者或处理者会否以及在多大程度上对违规进行通告；

i) 针对与同一主体相关事宜有关的控制者或处理者，此前被责令采取的第 58(2)条所述措施的情形，需遵守这些措施；

j) 遵守根据第 40 条核准的行为守则或根据第 42 条核准的认证机制；和

k) 适用于本案情形的任何其他加重或减缓处罚因素，如直接或间接因侵权而获得的经济利益或避免的损失。

3 若控制者或处理者有意或因过失违反本法规的若干规定，对于同一或有关联的处理操作，行政罚款总额不得超过最严重违规所规定的数额。

4 依照第 2 款的规定，违反下列规定的，将被处以最高达 1000 万欧元的行政罚款，或对企业处以上一财政年度全球年营业额总额的 2%以下的行政罚款，且以较高的数额为准:

a) 根据第 8 条、第 11 条、第 25 条至第 39 条、第 42 条和第 43 条规定，控制者和处理者的义务；

b) 根据第 42 条和第 43 条的规定，认证机构的义务；

c) 根据第 41 条第 4 款规定，监测机构的义务。

5 依照第 2 款的规定，违反下列规定的将被处以最高达 2000 万欧元的行政罚款，或就一项经营而言，最高可处以上一财政年度全球年营业额的 4%，两者以较高者为准：:

a) 根据第 5、6、7 和 9 条处理的基本原则，包括同意的条件；

b) 根据第 12 条至第 22 条规定的数据主体权利；

c) 根据第 44 至 49 条，将个人数据转交给第三国或国际组织的收件人；

d) 根据第 IX 章通过的成员国法律所规定的任何义务；

e) 不符合监督机构对处理或数据流中断的所发命令、临时或最终限制的，以及未能提供对第 58(1)条所述违规的访问权限的;

6 违反监督机构根据第 58 条第 2 款所发命令的，应当按照本条第 2 款，处以高达 2000 万欧元的行政罚款，或者就一项经营而言，最高可达前一财政年度全球年营业额的 4%，且以较高的数额为准。

7 在不损害监督机构由第 58 条第 2 款所赋予的纠正权的情况下，每个成员国可就对会员国所设的公权单位和机构，是否以及在何种程度上处以行政罚款，指定相应的规则。

8 在本条项下，监督机构权力的行使应根据欧盟和成员国的法律，遵守适当的程序保障，包括有效的司法救济和法定诉讼程序。

9 如果成员国的法律制度没有规定行政罚款，则本条的适用方式可使罚款由主管监督当局提出，并由国家主管法院实施，同时确保这些法律补救办法有效，并与监督当局的行政罚款具有同等效力。在任何情况下，所实施的罚款应是有效的、适当的和有惩戒性的。这些会员国应在 2018 年月 25 日前将其根据本款通过的法律的规定通知委员会，并·第一时间通知其后对其有影响的任何修正法或修正案。

第 84 条　处罚

1 成员国应制定适用于违反本法规的其他处罚的规则，特别是不符合第 83 条规定的行政处罚的违规行为，并应采取一切必要措施来确保其实施。这样的处罚应该是有效的、适当的和惩戒性的。

2 各成员国应于 2018 年 5 月 25 日之前，将其根据第 1 款通过的法律规定通知欧洲委员会，并将随后对其产生影响的任何修正案毫不拖延地通知委员会。

第九章. 特定数据处理情形下的相关规定

第 85 条　言论和信息的自由与处理

1 各会员国应根据本法规，将保护个人数据的权利与言论自由权和信息权相协调，包括为新闻目的而进行的处理以及学术、艺术或文学表达的目的。

2 对于进行新闻目的和学术、艺术或文学表达目的的处理，成员国应提供豁免或限制，具体参照第 II 章(原则)、第 III 章(数据主体的权利)，第 IV 章(控制者和处理者)，第 V 章(个人数据向第三国或国际组织转移)，第 VI 章(独立监督机构)，第 VII 章(合作和一致性)，且如需协调言论和信息自由权与个人数据保护之间的关系，参照第 IX 章(特定数据处理情况)。

3 每一成员国应向欧洲委员会通报其根据第 2 款所通过的法律规定，并及

时通报影响这些规定的任何后续修订法或修正案规定。

第 86 条　官方文件的处理以及公众获取

公共当局、公共机构或私人机构为公共利益而执行的任务持有的正式文件中的个人资料，可由公共当局或机构根据欧盟或成员国法律予以披露，以便使公众查阅官方文件的权利与根据本法规保护个人资料的权利相协调。

第 87 条　国家鉴定数据的处理

成员国可进一步确定处理国家身份证号码或一般用途的任何其他标识符的具体条件。在这种情况下，国家标识号或一般用途的任何其他标识符应仅适用于根据本法规对数据主体的权利和自由采取适当保障措施。

第 88 条　职场数据处理

1　成员国可以通过法律或集体协议规定更具体的规则，以确保对雇员工作方面的个人数据处理过程中的权利和自由的保护，特别是对于招聘的目的，雇佣合同的履行，包括免除由法律或集体协议规定的义务，工作的管理、计划和组织，工作场所中的平等和多样性，工作中的健康和安全，雇主或客户的产权保护，锻炼和享受的目的，在个人或集体的基础上，与雇佣相关的权利和福利，以及终止雇佣关系的目的。

2　这些规则应包括适当和具体的措施，以保障数据主体的人的尊严、合法利益和基本权利，特别是在处理的透明度、企业集团内部个人资料的转让、或在工作场所从事联合经济活动和监测系统的一群企业方面。

3　各成员国应在 2018 年 5 月 25 日之前，将其根据第 1 款所通过的法律条款通知欧洲委员会，并及时通报影响这些规定的任何后续修订法或修正案规定。

第 89 条　涉及公共利益、科学历史研究或者统计等目的的数据处理的保护与限制

1　为公众利益、科学、历史研究或统计目的而进行的数据处理，应按照本法规的规定，对数据主体的权利和自由进行适当的保障。这些保障措施应确保技术和组织措施的到位，特别是为了确保尊重数据最小化原则。这些措施可能包括化名，但前提是这些目的可以这种方式得以实现。如果这些目的可以被进一步的处理实现，但这些处理不允许或不再允许对数据主体进行识别，那么这些目的应以该种方式实现。

2 个人数据的处理是为科学、历史研究或统计目的处理的，欧盟或成员国法律可规定减损第 15、16、18 和 21 条所述权利，但须遵守本条第 1 款所述条件和保障措施，当这些权利可能使具体目的无法实现或对其造成严重损害时，为了实现这些目的这种减损是必要的。

3 出于公共权益归档目的的个人数据处理，欧盟或成员国法律，欧盟或成员国法律可规定减损第 15、16、18 和 21 条所述权利，但须遵守本条第 1 款所述条件和保障措施，当这些权利可能使具体目的无法实现或对其造成严重损害时，为了实现这些目的这种减损是必要的。

4 第 2 和第 3 款所述的处理在同时服务于另一目的时，该减损应只适用于这两款中所述目的的处理。

第 90 条　保密义务

1 成员国可通过具体规则，制定第 58 条第 1 款(e)和(f)项规定的关于控制者或处理者为主体时的监督机构权限，在欧盟成员国法律或由国家主管机构所设规定之下，建立专业保密的义务或其他同等保密义务，这对于个人数据保护权利和保密义务的协调是必要的且适当的。这些规则仅适用于控制者或处理者已在该保密义务所涵盖的活动中获得或已获得的个人数据。

2 各成员国应将根据第 1 款所采用的规则，于 2018 年 5 月 25 日之前通知欧洲委员会，并在不延误的情况下，对其进行后续修订。

第 91 条　教会与宗教协会现有的数据保护规则

1 本法案生效之时，在成员国、教堂和宗教团体或社区中应用关于处理自然人保护的综合规则，这些规则可能会继续适用，以协调使其符合本法案规定。

2 依照本条第 1 款规定应用综合规则的教会和宗教协会，应受独立监督机构的监督，该监督机构可能是特定的，但前提是它满足本法案第 VI 章规定的条件。

第十章. 委托行为与实施行为

第 92 条　委托权的行使

1 根据本条规定的条件，授予欧洲委员会通过授权法案的权力。

2 欧洲委员会将于 2016 年 5 月 24 日起的一段不确定的时期，被授予第 12 条第 8 款和第 43 条第 8 款所述权力的授予权。

3 第 12 条第 8 款和第 43 条第 8 款所述权力的授予权，可随时由欧洲议会或理事会撤销。撤销决定应终止该决定中所规定的权力授予权。在其发表于欧盟官方期刊之日或在其指定日期之后的第二天生效，但不得影响任何已生效授权的效力。

4 欧洲委员会一旦通过一项授权，应同时将其通知到欧洲议会和理事会。

5 根据第 12 条第 8 款和第 43 条第 8 款所通过的授权，将会立即生效，除非欧洲议会或理事会在为期三个月的通知期内，向欧洲议会和理事会表示反对意见，或如在该通知期满之前，欧洲议会和理事会均向欧洲委员会通知其反对意见。该期限能够在欧洲议会或理事会的倡议下延长 3 个月。

第 93 条　欧洲委员会程序

1 欧洲委员会应得到一个委员的协助。该委员应是第 182/2011 号法规(欧盟)规定范围内的委员。

2 对本条有引用之处，则须适用第 182/2011 号法规(欧盟)第 5 条。

3 对本条有引用之处，则应适用第 182/2011 号法规第 8 条，及其第 5 条。

第十一章. 最终条款

第 94 条　废除第 95/46/EC 号指令

1 法规 95/46/EC 自 2018 年 5 月 25 日起废止。

2 凡对废止法规的引用应被解释为对本法规的引用。关于依据第 95/46/EC 号法规第 29 条所建立的个人数据处理，对工作组关于个人保护的引用，应解释为对本规例所设立的欧洲资料保护委员会的提述。。

第 95 条　与第 2002/58/EC 号指令的关系

在处理欧盟内公共通讯网络中提供公开电子通讯服务相关事宜的过程中，本法案不得将额外义务强加于自然人或法人，在有关事宜上，则须遵从在指令 2002/58/EC 中所陈述的相同目标。

第 96 条　与先前缔结协定的关系

涉及向第三国或国际组织转让个人资料的国际协定于 2016 年月 24 日前由成员国缔结，并符合该日以前适用的欧盟法律的，在修订、更换或撤销之前应继续有效。

第 97 条　欧洲委员会报告

1　在 2020 年 5 月 25 日之前以及此后每四年，欧洲委员会应向欧洲议会和理事会提交一份关于本法案的评估和审查报告。该报告应当被公开。

2　在第 1 款所述的评价和审查范畴内，欧洲委员会应特别审查下列各项的适用和运作情况：

a) 关于向第三国或国际组织转移个人资料的第五章，特别是根据本法规第 45(3)条通过的决定和根据第 95/46/EC 号指令第 25(6)条通过的决定；

b) 关于合作和一致性的第七章。

3　为了第 1 款的目的，欧洲委员会可要求成员国和监督机构提供资料。

4　委员会在进行第 1 和第 2 款所述的评价和审查时，应考虑到欧洲议会、理事会和其他有关机构或来源的立场和结论。

5　欧洲委员会应在必要时提出适当的建议，以修正本法案，特别是考虑到信息技术的发展和信息社会的进展情况。

第 98 条　关于其他有关数据保护的欧盟法案的审查

欧洲委员会应酌情提交立法建议，以修订其他关于保护个人数据的联合法律行为，以确保在处理过程中对自然人进行统一和一致的保护。这尤其涉及与保护工会组织、机构、办事处和机构处理自然人有关的规则以及这些数据的自由流动。

第 99 条　生效及适用

1. 本法规自"欧洲欧盟期刊"公布后第二十天起生效。

2. 本法案将于 2018 年 5 月 25 日起适用。

本法规应具有全部约束力，并直接适用于所有成员国。

欧洲议会主席舒尔茨，委员会主席亨尼斯-普拉斯沙尔特修订于布鲁塞尔，2016。

——译文结束——

关于本译文的说明

本译文中未包括 GDPR 法案初始部分共计 173 段的法案立法说明。

介于时间以及非英语专业翻译等原因，对于译文中可能会出现的错漏之处，敬请谅解。

本译文所有内容仅供技术交流使用，学术研究或法律合规商用等诉求，请阅读英文原文（http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf）。本译文未经译制工作组许可，任何机构和个人请勿以任何形式翻版、复制、发表或引用。

GDPR 译制工作组

二〇一八年三月于北京