通用数据保护条例

经过欧盟议会长达四年的讨论，欧盟《通用数据保护条例》（General Data Protection Regulation，简称 GDPR）终于在 2018 年 5 月 25 日生效。

第一章 一般条款

第 1 条 主要事项与目标

1．本条例制定关于处理个人数据中对自然人进行保护的规则，以及个人数据自由流动的规则。

2．本条例保护自然人的基本权利与自由，特别是自然人享有的个人数据保护的权利。

3．不能以保护处理个人数据中的相关自然人为由，对欧盟内部个人数据的自由流动进行限制或禁止。

第 2 条 适用范围

1．本条例适用于全自动个人数据处理、半自动个人数据处理，以及形成或旨在形成用户画像的非自动个人数据处理。

2．本条例不适用以下情形：

(a)欧盟法管辖之外的活动中所进行的个人数据处理；

(b)欧盟成员国为履行《欧盟基本条约》（TEU）第 2 章第 5 款所规定的活动而进行的个人数据处理；

(c)自然人在纯粹个人或家庭活动中所进行的个人数据处理；

(d)）有关主管部门为预防、调查、侦查、起诉刑事犯罪、执行刑事处罚、防范及预防公共安全威胁而进行的个人数据处理。

3．欧盟机构、实体、办事处和规制机构所进行的个人数据处理，适用(EC)第45/2001 条例。根据本条例第 98 条，(EC)第 45/2001 条例和其他适用于此类个人数据处理的欧盟法案应当进行调整，以符合本条例的原则和规则。

4．本条例不影响 2000/31/EC 指令的适用，特别是 2000/31/EC 指令第 12 至 15 条所规定的中间服务商的责任规则的适用。

第 3 条 地域范围

1．本例适用于在欧盟内部设立的数据控制者或处理者对个人数据的处理，不论其实际数据处理行为是否在欧盟内进行。

2．本条例适用于如下相关活动中的个人数据处理，即使数据控制者或处理者不在欧盟设立：

(a)为欧盟内的数据主体提供商品或服务——不论此项商品或服务是否要求数据主体支付对价；或

(b)对发生在欧洲范围内的数据主体的活动进行监控。

3．本条例适用于在欧盟之外设立，但基于国际公法成员国的法律对其有管辖权的数据控制者的个人数据处理。

第 4 条 定义

就本条例而言：

(1)“个人数据”指的是任何已识别或可识别的自然人（“数据主体”）相关的信息；一个可识别的自然人是一个能够被直接或间接识别的个体，特别是通过诸如姓名、身份编号、地址数据、网上标识或者自然人所特有的一项或多项的身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份而识别个体。

(2) “处理” 是指任何一项或多项针对单一个人数据或系列个人数据所进行的操作行为，不论该操作行为是否采取收集、记录、组织、构造、存储、调整、更改、检索、咨询、使用、通过传输而公开、散布或其他方式对他人公开、排列或组合、限制、删除或销毁而公开等自动化方式。

(3) “限制处理” 是指对存储的个人数据进行标记，以限制此后对该数据的处理行为。

(4) “用户画像” 指的是为了评估自然人的某些条件而对个人数据进行的任何自动化处理，特别是为了评估自然人的工作表现、经济状况、健康、个人偏好、兴趣、可靠性、行为方式、位置或行踪而进行的处理。

(5) “匿名化” 指的是在采取某种方式对个人数据进行处理后，如果没有额外的信息就不能识别数据主体的处理方式。此类额外信息应当单独保存，并且已有技术与组织方式确保个人数据不能关联到某个已识别或可识别的自然人。

(6) “档案系统” 指的是根据某种特定标准——不论这种标准是去中心化的、分散的、功能性的或是基于地理而设置的——而可以访问的个人数据的结构化集合。

(7) “控制者” 指的是那些决定——不论是单独决定还是共同决定——个人数据处理目的与方式的自然人或法人、公共机构、规制机构或其他实体；如果此类处理的方式是由欧盟或成员国的法律决定的，那么对控制者的定义或确定控制者的标准应当由欧盟或成员国的法律来规定。

(8) “处理者” 指的是为数据控制者而处理个人数据的自然人或法人、公共机构、规制机构或其他实体。

(9) “接收者” 指的是接收数据的自然人、法人、公共机构、规制机构或另一实体，不论其是否为第三方。然而，公共机构基于欧盟或成员国法律的某项特定调查框架而接收个人数据，则不应当被视为接收者；公共机构对此类数据的处理，应当根据处理目的遵循可适用的数据保护规则。

(10) “第三方” 指的是除了数据主体、控制者、处理者、控制者或处理者直接授权其处理个人数据之外的自然人或法人、公共机构、规制机构或组织。

(11)数据主体的 “同意” 指的是数据主体通过一个声明，或者通过某项清晰的确信行动而自由作出的、充分知悉的、不含混的、表明同意对其相关个人数据进行处理的意愿。

(12) “个人数据泄露” 是指由于违反安全政策而导致传输、储存、处理中的个人数据被意外或非法损毁、丢失、更改或未经同意而被公开或访问。

(13) “基因数据” 指的是和自然人的遗传性或获得性基因特征相关的个人数据，这些数据可以提供自然人生理或健康的独特信息，尤其是通过对自然人生物性样本进行分析而可以得出的独特信息。

(14) “生物性识别数据” 指的是基于特别技术处理自然人的相关身体、生理或行为特征而得出的个人数据，这种个人数据能够识别或确定自然人的独特标识，例如脸部形象或指纹数据。

(15) “和健康相关的数据” 指的是那些和自然人的身体或精神健康相关的、显示其个人健康状况信息的个人数据，包括和卫生保健服务相关的服务。

(16) “主要营业机构” 指的是：

(a)如果控制者在不止一个成员国内有多处营业机构，那么其在欧盟的管理中心所在地是主要营业机构，除非个人数据处理的目的与方式是由控制者的另一个

机构决定的，并且这一机构有权实施此决定，在这种情况下，做出此类决定的机构应当被认为是主要营业机构；

(b)如果处理者在不止一个成员国内具有多处机构，那么其在欧盟的管理中心所在地是主要营业机构。如果处理者在欧盟没有管理中心，那么在处理者需要遵守本条例所规定的特殊责任的前提下，其在欧盟的主要处理活动发生地的机构应当被视为主要营业机构。

(17) “代表” 指的是控制者或处理者根据第 27 条在欧盟书面委任，代表控制者或处理者承担本条例所规定的相应责任的自然人或法人。

(18) “经济主体” 的含义是采用任意法律形式的进行经济活动的自然人或法人，包括经常进行经济活动的合伙企业或协会；

(19) “企业集团” 的含义是控股企业和被控股企业；

(20) “有约束力的公司规则” 指的是在某成员国内设立的控制者或处理者，为了在企业集团内部或进行联合经济活动的经济主体内部将个人数据转移或多次转移给位于第三国或多个第三国的控制者或处理者，所遵循的个人数据保护政策。

(21) “监管机构” 指的是成员国根据第 51 条而设立的独立性公共机构。

(22)

(a)控制者或处理者是在某监管机构所在的成员国的境内所设立的；

(b)数据处理对居住在某监管机构所在地成员国的数据主体具有实质性影响；或者

(c)该监管机构已经收到一项申诉；

(23) “跨境处理” 指的是：

(a)个人数据处理发生在一个控制者或处理者在多个成员国所设立的多个营业机构内；或者

(b)个人数据处理是在欧盟内的控制者或处理者的单一营业机构内进行的，但其对不止一国的数据主体具有实质性影响。

(24) “相关和合理的异议” 指的是对是否存在违反本条例的情形，或者某项和控制者或处理者相关的初步设想是否符合本条例的异议——已有证据表明，这种初步设想的决定会对数据主体的基本权利和自由，以及在某些情形下对欧盟的个人数据的自由流通会带来风险。

(25) “信息社会服务” 指的是欧洲议会和欧盟理事会的(EU) 2015/1535 指令在第1（1）条（b）点所定义的服务。

(26) “国际组织” 指的是依照国际公法、或根据两个或多个国家协议所设立的组织及其下属机构。

1．本例适用于在欧盟内部设立的数据控制者或处理者对个人数据的处理，不论其实际数据处理行为是否在欧盟内进行。

2．本条例适用于如下相关活动中的个人数据处理，即使数据控制者或处理者不在欧盟设立：

(a)为欧盟内的数据主体提供商品或服务——不论此项商品或服务是否要求数据主体支付对价；或

(b)对发生在欧洲范围内的数据主体的活动进行监控。

3．本条例适用于在欧盟之外设立，但基于国际公法成员国的法律对其有管辖权的数据控制者的个人数据处理。

第二章 原则

第 5 条 个人数据处理原则

1．对于个人数据，应遵循下列规定：

(a)对涉及到数据主体的个人数据，应当以合法的、合理的和透明的方式来进行处理（“合法性、合理性和透明性”）；

(b)个人数据的收集应当具有具体的、清晰的和正当的目的，对个人数据的处理不应当违反初始目的。根据第 89（1）条，因为公共利益、科学或历史研究或统计目的而进一步处理数据，不视为违反初始目的（“目的限制”）；

(c)个人数据的处理应当是为了实现数据处理目的而适当的、相关的和必要的（“数据最小化”）；

(d)个人数据应当是准确的，如有必要，必须及时更新；必须采取合理措施确保不准确的个人数据，即违反初始目的的个人数据，及时得到擦除或更正（“准确性”）；

(e)对于能够识别数据主体的个人数据，其储存时间不得超过实现其处理目的所必需的时间；超过此期限的数据处理只有在如下情况下才能被允许：为了实现公共利益、科学或历史研究目的或统计目的，为了保障数据主体的权利和自由，并采取了本条例第 89（1）条所规定的合理技术与组织措施。（“限期储存”）；

(f) 处理过程中应确保个人数据的安全，采取合理的技术手段、组织措施，避免数据未经授权即被处理或遭到非法处理，避免数据发生意外毁损或灭失（“数据的完整性与保密性”）。

2．控制者有责任遵守以上第 1 段，并且有责任对此提供证明。（“可问责性”）。

第 6 条 处理的合法性

1．只有满足至少如下一项条件时，处理才是合法的，且处理的合法性只限于满足条件内的处理：

(a)数据主体已经同意基于一项或多项目的而对其个人数据进行处理；

(b)处理对于完成某项数据主体所参与的契约是必要的，或者在签订契约前基于数据主体的请求而进行的处理；

(c) 处理是控制商履行其法定义务所必需的；

(d)处理对于保护数据主体或另一个自然人的核心利益所必要的；

(e)处理是数据控制者为了公共利益或基于官方权威而履行某项任务而进行的；

(f)处理对于控制者或第三方所追求的正当利益是必要的，这不包括需要通过个人数据保护以实现数据主体的优先性利益或基本权利与自由，特别是儿童的优先性利益或基本权利与自由。

第 1 段（f）点不适用公共机构在履行其任务时的处理。

2．对于第 1 段（c）和（e）所规定的处理，成员国可以维持或新制定更多具体条款，以适应本条例规则的适用，成员国为了确保合法与合理处理，可以制定更为明确的规定，包括第 9 章所规定的其他特定的处理情形。

3．第 1 段（c）和（e）所规定的处理的基准应当通过如下法律进行规定：

(a)欧盟法；或者

(b)控制者所属的成员国的法律。

处理的目的应当在此法律基准上进行确定，而对于第 1 段（e）所规定的处理，处理的目的应当是控制者为了公共利益或基于官方权威而履行某项任务。此法律基准可以包含如下特定条款，以适应对本条例规则的适用：对控制者处理的

合法性进行监控的一般条件；可以被处理的数据类型；相关数据主体；个人数据公开的目的，以及其可能被公开给的对象；目的限定；储存期限；包括第 9 章所规定的其他特定的处理情形在内的处理操作和处理程序。欧盟或成员国的法律应当满足公共利益的目标，且应当与实现正当目的成比例。

4．若处理是出于收集个人数据以外的其他目的，如果该目的未经数据主体同意或并非是基于联盟或成员国的法律（在一个民主社会中，若要实现第 23（1）条中的目的，法律是必要且合适的），那么为确保该目的与初始目相容，控制商应当考虑以下因素，但不限于以下因素：

(a)个人数据收集时的目的与计划进一步处理的目的之间的所有关联性；

(b)个人数据收集时的语境，特别是数据主体与控制者之间的关系；

(c)个人数据的性质，特别是某些特定类型的个人数据是否符合第 9 条的规定，或者与刑事定罪和刑事违法相关的个人数据是否符合第 10 条的规定；

(d) 数据主体计划进一步处理可能造成的结果；

(e)是否具有加密与匿名化措施等恰当保护措施；

第 7 条 同意的条件

1．当处理是建立在同意基础上的，控制者需要能证明，数据主体已经同意对其个人数据进行处理。

2．如果数据主体的同意是在涉及到其他事项的书面声明的情形下作出的，请求获得同意应当完全区别于其他事项，并且应当以一种容易理解的形式，使用清晰和平白的语言。任何违反本条例的声明都不具有约束力。

3．数据主体应当有权随时撤回其同意。在撤回之前，对于基于同意的处理，其合法性不受影响。在数据主体表达同意之前，数据主体应当被告知这点。撤回同意应当和表达同意一样简单。

4．分析同意是否是自由做出的，应当最大限度地考虑一点是：对契约的履行——包括履行条款所规定的服务——是否要求同意履行契约所不必要的个人数据处理。

第 8 条 信息社会服务中适用儿童同意的条件

1．在第 6（1）条（a）适用的情形下，对于为儿童直接提供信息社会服务的请求，当儿童年满 16 周岁，对儿童个人数据的处理是合法的。当儿童不满 16 周岁，只有当对儿童具有父母监护责任的主体同意或授权，此类处理才是合法的。

2．对于年满 13 周岁的情形，成员国的法律可以降低年龄要求。

3．控制者应当采取合理的努力，结合技术可行性，确保此类情形中对儿童具有父母监护责任的主体已经授权或同意。

第 1 段不应影响成员国的一般合同法，例如关于儿童的合同有效性、形成与效力的规则。

第 9 条 对特殊类型个人数据的处理

1．对于那些显示种族或民族背景、政治观念、宗教或哲学信仰或工会成员的个人数据、基因数据、为了特定识别自然人的生物性识别数据、以及和自然人健康、个人性生活或性取向相关的数据，应当禁止处理。

2．如果具有如下条件之一，第 1 段将不适用：

(a)数据主体明确同意基于一个或多个特定目的而授权处理其个人数据，但依照欧盟或成员国的法律规定，数据主体无权解除第 1 段中所规定的禁令的除外；

(b)处理对于控制者履行责任以及行使其特定权利是必要的，或者对于在雇佣、社会安全与社会保障法领域采取符合欧盟或成员国法律或集体协议的措施以保护数据主体的根本权利和利益是必要的；

(c)数据主体因为身体原因或法律原因而无法表达同意，但处理对于保护数据主体或另一自然人的核心利益却是必要的；

(d)基金、协会或其它具有政治、哲学、宗教或工会目的的非盈利机构的正当性活动中所进行的处理，并且已经采取了恰当的保护措施；或者处理目的仅仅和机构成员、之前成员或具有经常联系的人相关，并且个人数据在未经数据主体同意前不对实体外的人公开；

(e)对数据主体已经明显公开的相关个人数据的处理；

(f)当处理对于提起、行使或辩护法律性主张必要时，或者法院在其所有的司法活动中所进行的处理；

(g)处理对实现实质性的公共利益必要的，建立在欧盟或成员国的法律基准之上、对实现目标是相称的，尊重数据保护权的核心要素，并且为数据主体的基本权利和利益提供合适和特定的保护措施；

(h)处理对于预防性医学或临床医学目的是必要的，或者对于评估雇员的工作能力、医疗诊断、提供——基于欧盟或成员国法律，或遵循和健康职业机构签订的契约并遵循第 3 段所规定的情形与保障措施——健康或社会保健或治疗或管理健康或社会保健体系是必要的；

(i)在公共健康领域，处理是为了实现公共利益所必要的，例如，在欧盟或成员国内已经为保障数据主体的权利与自由而采取合适与特定措施的法律基础上，处理对于预防严重的跨境健康威胁是必要的，或者为了保障医疗质量和安全、医疗产品或医疗设备的高质量和安全是必要的；或者

(j)处理对于实现符合第 89(1)条公共利益、科学或历史研究目的或统计目的是必要的，处理采取了与其期望目的所相称的处理，尊重数据保护权的核心要素，并且对数据主体的基本权利与利益采取了合适与特定的措施。

3．根据欧盟或成员国的有权机构所制定的法律或规则而具有保守职业性秘密责任的职业主体，或者根据欧盟或成员国的有权机构所制定的法律或规则而具有保守秘密责任的自然人，可以为了第 2 段（h）点所规定的目的而处理第 1 段所规定的个人数据。

4．对于基因数据、生物性识别数据或健康相关数据的处理，成员国可以维持原有规定，或者作出新的规定，包括对处理基因数据、生物性识别数据或健康相关数据进行限定。

第 10 条 处理涉及犯罪定罪与违法的个人数据

处理和犯罪定罪与违法相关的个人数据，或处理第 6（1）条规定的与安全措施相关的个人数据，只有如下情形才能被允许：当个人数据处理为官方机构控制，或者当欧盟或成员国的法律授权进行处理，并且采取了恰当的措施保障数据主体的权利与自由。任何犯罪定罪的全面性登记只能由官方机构进行。

第 11 条 不需要识别的处理

1．如果控制者处理个人数据的目的不需要或不再需要控制者对数据主体进行识别，控制者就不再具有为了遵循本条例而维持、获取或处理额外信息以识别数据主体的责任。

2．对于第 1 段所规定的情形，如果控制者能够证明其不适合识别数据主体，如有可能，数据控制者应当告知数据主体。在此类情形下，除非数据主体为了行使第 15 至 20 条所规定的权利，需要提供额外信息而使得对其识别变得可能，第 15 至 20 条将不应适用。

第三章 数据主体的权利

第一部分 透明性与模式

第 12 条 信息、交流与模式的透明性——保证数据主体权利的行使

1．对于和个人信息处理相关的第 13 和第 14 条规定的所有信息、或者第 15 条至 22 条以及 34 条所规定的所有交流，控制者应当以一种简洁、透明、易懂和容易获取的形式，以清晰和平白的语言来提供；对于针对儿童的所有信息，尤其应当如此。信息应当以书面形式或其他形式提供，包括在合适的情况下通过电子方式提供。若数据主体的身份可通过其他途径得到证实，那么控制者可依主体申请以口头方式提供相关信息。

2．控制者应当对数据主体行使第 15 至 22 条的权利而提供帮助。对于第 11（2）条所规定的情形，当数据主体请求其行使第 15 至 22 条的权利，控制者不应拒绝，除非控制者能够证明其并不适宜识别数据主体。

3．在数据主体根据第 15 至 22 条的规定提出请求后，控制者应当提供信息，不应无故拖延，在任何情形下应当在收到请求后一个月内提供信息。在必要的情形下，考虑到请求的复杂性和多样性，这个期限可以再延长两个月。如果有

此类延长，控制者应当在收到请求的一个月内将此类延长以及延长原因告知数据主体。当数据主体以电子形式做出请求，在可行的情况下，对信息的提供也应当以电子形式提供，除非数据主体有不同请求。

4．如果控制者没有采取相应的行动对数据主体的请求做出回应，那么应当及时告知该数据主体其在收到请求后一个月内未能采取行动的具体原因，同时可向监管机构提出申诉，寻求司法救济。

5．第 13 和第 14 条所规定的信息以及第 15 至 22 条和 34 条所规定的所有交流与行为都应当是免费的。当数据主体的请求明显不具备正当理由或超过必要限度，特别是当请求是重复性的时候，控制者可以：

(a)结合提供信息、交流或相应行动的行政花费，收取一定的合理费用；或者

(b)拒绝对请求作出行动。

控制者有责任证明数据主体的请求明显是毫无根据的或过分的。

6．在不影响第 11 条的前提下，控制者可以对第 15 至 21 条中提出要求的自然人的身份有合理怀疑，要求数据主体提供必要的额外信息以确认数据主体的身份。

7．根据第 13 条和 14 条提供给数据主体的信息可以和标准化的图标一起提供，以便于数据主体以一种一目了然的、易懂的和清晰的方式对计划的数据处理有全盘理解。当图标以电子化的方式提供，它们必须是机器可读的。

8．对于确定图标所提供的信息以及提供标准化图标的程序，欧盟理事会将有权根据第 92 条制定授权行动。

第二部分 信息与对个人数据的访问

第 13 条 收集数据主体个人数据时应当提供的信息

1．当收集和数据主体相关的个人数据时，控制者应当为数据主体提供如下信息：

(a)控制者的身份与详细联系方式，以及如果适用的话，控制者的代表；

(b)数据保护官的详细联系方式，如果适用的话；

(c)处理将要涉及到的个人数据的目的，以及处理的法律基础；

(d)当处理是基于（f）点或第 6（1）条的时候，控制者或第三方的正当利益；

(e)个人数据的接收者或者接收者的类型，如果有的话；

(f)如果适用的话，控制者期望将数据转移到第三国或国际组织的事实、欧盟委员会作出或未作出充分决定的事实，或者，在第 46 或 47 条或者第 49（1）条的第二小段所规定的转移情形中，所采取的适当保障措施的参考资料、获取它们备份的方式，或者在那里可以获取它们。

2．除了第 1 段所规定的信息，控制者应当在获取个人数据时为数据主体提供确保合理与透明处理所必要的进一步信息：

(a)个人数据将被储存的期限，以及确定此期限的标准；

(b)数据主体所拥有的权利：可以要求控制者提供对个人数据的访问、更正或擦除，或者限制或反对相关处理的权利；数据携带权；

(c)当处理是根据第 6（1）条或第 9（2）条的（a）点而进行的，数据主体拥有可以随时撤回——这种撤回不会影响撤回之前根据同意而进行处理的合法性——同意的权利；

(d)向监管机构进行申诉的权利；

(e)提供个人数据是一项制定法还是合同法的要求，是否对于缔结一项契约是必要的，数据主体是否有责任提供个人数据，以及没有提供此类数据会造成的可能后果。

(f)存在自动化的决策，包括第 22（1）和（4）条所规定的用户画像，以及在此类情形下，对于相关逻辑、包括此类处理对于数据主体的预期后果的有效信息。

3．若控制者进一步处理个人信息的目的与收集个人信息的目的不一致，那么，控制者应当在进一步处理之前向数据主体提供此类目的的信息，以及提供第 2 段所规定的相关进一步信息。

4．在数据主体已经拥有信息的情况下，第 1，2，3 段不应当适用。

第 14 条 未获得数据主体个人数据的情形下，应当提供的信息

1．当个人数据还没有从数据主体那里收集，控制者应当向数据主体提供如下信息：

(a)控制者的身份与详细联系方式，以及如果适用的话，控制者的代表；

(b)如果适用的话，数据保护官的详细联系方式；

(c)处理将要涉及到的个人数据的目的，以及处理的法律基础；

(d)相关个人数据的类型；

(e)个人数据的接收者或者接收者的类型，如果有的话；

(f)如果适用的话，控制者期望将数据转移到第三国或国际组织、欧盟委员会作出或未作出的充足保护的认定，或者，在第 46 或 47 条或者第 49（1）条的第二小段所规定的转移情形中，所采取的适当保障措施的参考资料、获取它们备份的方式，或者在那里可以获取它们。

2．除了第 1 段所规定的信息，控制者应当向数据主体提供如下确保涉及到数据主体的处理是合理与透明的必要信息：

(a)个人数据将被储存的期限，或者如果不可能的话，用来确定此期限的标准；

(b)当处理是根据第 6（1）条（f）点而进行的，控制者或第三方所追求的正当利益；

(c)数据主体存在如下权利，可以要求控制者提供对个人数据的访问、更正或擦除，或者限制或反对相关处理，数据携带权；

(d)当处理是根据第 6（1）条或第 9（2）条的（a）点而进行的，数据主体拥有可以随时撤回——这种撤回不会影响撤回之前根据同意而进行处理的合法性——同意的权利；

(e)向监管机构进行申诉的权利；

(f)个人数据的来源，以及如果适用的话，其来源是否可以是公开性的资源；

(g)存在自动化的决策，包括第 22（1）和（4）条所规定的用户画像，以及在此类情形下，对于相关逻辑、包括此类处理对于数据主体的预期后果的有效信息。

3．控制者应当按如下方式提供第 1 段和第 2 段所规定的信息：

(a)应当在获得个人数据后的一段合理期限内提供信息，如果考虑到个人数据处理的特定情形，应当至少在一个月以内；

(b)如果个人数据是被用来和数据主体进行沟通的，最晚应当在其和数据主体进行第一次沟通时提供信息；

(c)如果个人数据将被计划披露给另一个接收者，那么最晚应当在个人数据被第一次披露时提供信息。

4．当控制者因为与收集个人信息时不一致的目的进一步处理个人信息，控制者应当在进一步处理之前向数据主体提供此类目的的信息，以及提供第 2 段所规定的相关进一步信息。

5．在如下情形中，第 1 至 4 段不适用：

(a)数据主体已经拥有信息；

(b)此类信息的提供是不可能的，或者说需要付出某种不相称的工作，在如下情形中尤其不适用：为了实现公共利益、科学或历史研究目的或统计目的，为了保障数据主体的权利和自由，并采取了本条例第 89（1）条所规定的合理技术与组织措施；或者本条第 1 段所规定的责任会严重妨碍实现处理的目标。在此类情形中，控制者应当采取恰当的措施保护数据主体的权利与自由与正当利益，包括使得信息可以公开获取；

(c)欧盟或成员国为控制者特别制定了获取或公开信息的法律，并且已经对保护数据主体的正当利益制定了恰当的措施；

(d)当个人数据必须保密，必须遵守欧盟或成员国法律所规定的职业秘密责任，包括制定法上的保守秘密责任。

第 15 条 数据主体的访问权

1．数据主体应当有权从控制者那里得知，关于其的个人数据是否正在被处理，如果正在被处理的话，其应当有权访问个人数据和获知如下信息：

(a)处理的目的；

(b)相关个人数据的类型；

(c)个人数据已经被或将被披露给接收者或接收者的类型，特别是当接收者属于第三国或国际组织时；

(d)在可能的情形下，个人数据将被储存的预期期限，或者如果不可能的话，确定此期限的标准；

(e)数据主体要求控制者纠正或擦除个人数据、限制或反对对数据主体相关的个人数据进行处理的权利；

(f)向监管机构进行申诉的权利；

(g)当个人数据不是从数据主体那里收集的，关于来源的任何信息；

(h)存在自动化的决策，包括第 22（1）和（4）条所规定的数据分析，以及在此类情形下，对于相关逻辑、包括此类处理对于数据主体的预期后果的有效信息。

2．当个人数据被转移到第三国或一个国际组织，数据主体应当有权获知和转移相关的符合第 46 条的恰当的保障措施。

3．控制者应当对进行处理的个人数据提供一份备份。对于任何数据主体所要求的额外备份，控制者可以根据管理花费而收取合理的费用。当数据主体通过电子方式而请求，且除非数据主体有其他请求，信息应当以通常使用的电子形式提供。

4．获取第三段中所规定的备份的权利不应当对他人的权利与自由产生负面影响。

第三部分 更正与擦除

第 16 条 更正权

数据主体应当有权从控制者那里及时得知对与其相关的不正确信息的更正。在考虑处理目的的前提下，数据主体应当有权完善不充分的个人数据，包括通过提供额外声明的方式来进行完善。

第 17 条 擦除权（“被遗忘权”）

1．数据主体有权要求控制者擦除关于其个人数据的权利，当具有如下情形之一时，控制者有责任及时擦除个人数据：

(a)个人数据对于实现其被收集或处理的相关目的不再必要；

(b)处理是根据第 6（1）条（a）点，或者第 9（2）条（a）点而进行的，并且没有处理的其他法律根据，数据主体撤回在此类处理中的同意；

(c)数据主体反对根据第 21（1）条进行的处理，并且没有压倒性的正当理由可以进行处理，或者数据主体反对根据第 21（2）条进行的处理；

(d)已经存在非法的个人数据处理；

(e)为了履行欧盟或成员国法律为控制者所设定的法律责任，个人数据需要被擦除；

(f)已经收集了第 8（1）条所规定的和提供信息社会服务相关的个人人数据。

2．当控制者已经公开个人数据，并且负有第 1 段所规定的擦除个人数据的责任，控制者应当考虑可行技术与执行成本，采取包括技术措施在内的合理措施告知正在处理个人数据的控制者们，数据主体已经要求他们擦除那些和个人数据相关的链接、备份或复制。

3．当处理对于如下目的是必要的，第 1 和第 2 段将不适用：

(a)为了行使表达自由和信息自由的权利；

(b)控制者执行或者为了执行基于公共利益的某项任务，或者基于被授予的官方权威而履行某项任务，欧盟或成员国的法律要求进行处理，以便履行其法律职责；

(c)为了实现公共健康领域符合第 9（2）条（h）和（i）点以及第 9（3）条的公共利益而进行的处理；

(d)如果第 1 段所提到权利会受严重影响，或者会彻底阻碍实现第 89(1)条的公共利益目的、科学或历史研究目的或统计目的；或者

(e)为了提起、行使或辩护法律性主张。

第 18 条 限制处理权

1．当存在如下情形之一时，数据主体有权要求控制者对处理进行限制：

(a)数据主体对个人数据的准确性有争议，并给与控制者以一定的期限以核实个人数据的准确性；

(b)处理是非法的，并且数据主体反对擦除个人数据，要求对使用其个人数据进行限制；

(c)控制者不再需要个人数据以实现其处理的目的，但数据主体为了提起、行使或辩护法律性主张而需要该个人数据；

(d)数据主体根据第 21（1）条的规定而反对处理，因其需要确定控制者的正当理由是否优先于数据主体的正当理由。

2．当处理受第 1 段的规定所限制，除了储存的情形，此类个人数据只有在如下情形中才能进行处理：获取了数据主体的同意，或者为了提起、行使或辩护法律性主张，或者为了保护另一个自然人或法人的权利，或者为了欧盟或某个成员国的重要公共利益。

3．那些根据第 1 段规定已经获取了对处理进行限制的数据主体，在限制被解除前，控制者应当告知数据主体。

第 19 条 关于更正或擦除或限制处理中的通知责任

对于所有根据第 16、17（1）、18 条而限制或擦除个人数据，或限制处理个人数据，控制者都应当将其告知个人数据已经被披露给的每个接收者——除非此类告知是不可能的，或者需要付出不相称的工作。如果数据主体提出要求，控制者应当将关于接收者的情形告知数据主体。

第 20 条 数据携带权

1．当存在如下情形时，数据主体有权获得其提供给控制者的相关个人数据，且其获得个人数据应当是经过整理的、普遍使用的和机器可读的，数据主体有权无障碍地将此类数据从其提供给的控制者那里传输给给另一个控制者：

(a)处理是建立在第 6（1）条（a）点或 9（2）条（a）点所规定的同意，或者 6（1）条所规定的合同的基础上的；

(b)处理是通过自动化方式的。

2．在行使第 1 段所规定的携带权时，如果技术可行，数据主体应当有权将个人数据直接从一个控制者传输到另一个控制者。

3．行使第 1 段所规定的权利，不能影响第 17 条的规定。对于控制者为了公共利益，或者为了行使其被授权的官方权威而进行的必要处理，这种权利不适用。

4．第 1 段所规定的权利不能对他人的权利或自由产生负面影响。

第四部分 反对的权利和自动化的个人决策

第 21 条 反对权

1．对于根据第 6（1）条（e）或（f）点而进行的关乎数据主体的数据处理，包括根据这些条款而进行的用户画像，数据主体应当有权随时反对。此时，控制者须立即停止针对这部分个人数据的处理行为，除非控制者证明，相比数据

主体的利益、权利和自由，具有压倒性的正当理由需要进行处理，或者处理是为了提起、行使或辩护法律性主张。

2．当因为直接营销目的而处理个人数据，数据主体有权随时反对为了此类营销而处理相关个人数据，包括反对和此类直接营销相关的用户画像。

3．当数据主体反对为了直接营销目的而处理，将不能为了此类目的而处理个人数据。

4．至晚在和数据主体所进行的第一次沟通中，第 1 段和第 2 段所规定的权利应当让数据主体明确知晓，且应当与其他信息区分开来，清晰地告知数据主体。

5．在适用信息社会服务的语境中，尽管存在 2002/58/EC 指令的规定，数据主体仍可以使用技术性条件、通过自动化方式行使反对权。

6．当个人数据是为了第 89（1）条所规定的科学目的或历史研究目的或统计目的，数据主体基于其特定情形应当有权反对对关乎其的个人数据进行处理，除非处理对于实现公共利益的某项任务是必要的。

第 22 条 自动化的个人决策，包括用户画像

1．数据主体有权反对此类决策：完全依靠自动化处理——包括用户画像——对对数据主体做出具有法律影响或类似严重影响的决策。

2．当决策存在如下情形时，第 1 段不适用：

(a)当决策对于数据主体与数据控制者的合同签订或合同履行是必要的；

(b)当决策是欧盟或成员国的法律所授权的，控制者是决策的主体，并且已经制定了恰当的措施保证数据主体的权利、自由与正当利益；或者

(c)当决策建立在数据主体的明确同意基础之上。

3．在第 2 段所规定的（a）和（c）点的情形中，数据控制者应当采取适当措施保障数据主体的权利、自由、正当利益，以及数据主体对控制者进行人工干涉，以便表达其观点和对决策进行异议的基本权利。

4．第 2 段所规定的决策的基础不适用于第 9（1）条所规定的特定类型的个人数据，除非符合第 9（2）条（a）点或（g）点的规定，并且已经采取了保护数据主体权利、自由与正当利益的措施。

第五部分限制

第 23 条 限制

1．若控制者或处理者受欧盟法律或某成员国法律的调整，那么欧盟法律或该成员国法律可以通过立法手段限制第 12 至 22 条、34 条以及第 5 条所赋予的责任范围与权利范围，只要其法律条款和第 12 至 22 条所赋予的责任与权利相对应。如果此类限制尊重基本权利与自由的核心要素，并且此类限制是实现如下民主社会中的目的所必要和成比例的措施，那么此类限制应当被允许：

(a)国家安全；

(b)国防；

(c)公共安全；

(d)预防、调查、侦查、起诉刑事违法进行或者执行刑法，包括保障公共安全和预防对公共安全的威胁；

(e)其他些欧盟或某个成员国的重要一般公共利益，特别是欧盟或某个成员国的经济或金融利益，包括财政、预算、税收事项、公共健康和社会安全；

(f)司法独立和司法诉讼的保护；

(g)为了规制性职业而预防、调查、保护和起诉违反伦理的行为；

(h)和行使（a）（b）（c）（d）（e）（g）点中所规定的官方权威相联系的某项监控、调查或规制功能；

(i)保护数据主体或其他人的权利和自由；

(j)实施民事法律主张。

2．需要特别注意的是，至少在涉及到如下情形时，任何第 1 段所规定的立法措施都应当包含特定条款，规定：

(a)处理的目的或处理的类型；

(b)个人数据的类型；

(c)施加限制的范围；

(d)防止滥用或非法性访问或转移的措施；

(e)控制者的具体情况或控制者类型的具体情况；

(f)在考虑了处理的性质、范围和目的或处理类型之后所制定的储存期限和可适用的保障措施；

(g)数据主体的权利和自由所面临的风险；以及

(h)数据主体获知限制的权利，除非这种权利可能影响实现限制的目的。

第四章 控制者和处理者

第一部分 一般性责任

第 24 条 控制者的责任

1．在考虑了处理的性质、范围、语境与目的，以及考虑了处理对自然人权利与自由所带来的不同概率和程度的风险后，控制者应当采取恰当的技术与组织措施，保证处理符合本条例规定的，并且能够证明处理符合本条例规定。必要时，这些措施应当被审查。

2．第 1 段所规定的措施，当和处理活动成比例时，应当包括控制者所采用的合适的数据保护政策。

3．遵守第 40 条所规定的已生效的行为准则，或遵守第 42 条规定的已生效的认证机制，这可以被用以证明控制者责任的合规性。

第 25 条 通过设计的数据保护和默认的数据保护

1．在考虑了最新水平、实施成本、处理的性质、处理的范围、处理的语境与目的，以及处理给自然人权利与自由带来的伤害可能性与严重性之后，控制者应当在决定处理方式时和决定处理时，应当采取合适的技术与组织措施，并且在处理中整合必要的保障措施，以便符合本条例的要求和保护数据主体的权利。例如，控制者可以采取匿名化，一种设计用来实施数据保护原则——比如数据最小化原则——的措施。

2．控制者有责任采取适当的技术与组织措施，以保障在默认情况下，只有某个特定处理目的所必要的个人数据被处理。这种责任适用于收集的个人数据的数量、处理的限度，储存的期限以及可访问性。尤其需要注意的是，此类措施必须确保，在默认情况下，如果没有个体介入，个人数据不能为不特定数量的自然人所访问。

3．根据第 42 条的某种已生效的认证机制，可以被用来证明本条第 1 段和第 2 段所规定的合规要求。

第 26 条 共同控制者

1．当两个或更多控制者联合确定处理的目的与方法，它们就是共同控制者。它们应当以一种透明的方式确定遵守本条例责任的相应责任，尤其当其涉及到行使数据主体个人权利，以及涉及控制者为数据主体——根据他们的合约安排—

—提供第 13 条和第 14 条所规定的信息的相应责任，除非欧盟或成员国的法律已经对对控制者施加了相应责任。

2．第 1 段所规定的合约安排应当恰当地反映相对于数据主体的共同控制者的相应角色和相互关系。数据主体应当可以知晓安排的实质。

3．不论第 1 段所规定的合约安排的条款如何，数据主体都可以向任一控制者主张其本条例所赋予的权利。

第 27 条 不在欧盟所设立的控制者或处理者的代表

1．在第 3（2）条适用的情形下，控制者或处理者应当以书面形式在欧盟委任一名代表。

2．此项责任不应当适用于：

(a)除了第 9（1）条所规定的特定类型数据的大规模处理，或者第 10 条所规定的和刑事定罪或违法相关的个人数据处理之外的偶尔性处理，以及考虑到处理的性质、语境、范围和目的，不太可能对自然人的权利与自由带来风险的处理；或者

(b)公共机构或实体。

3．为数据主体提供相关商品或服务，或者监控数据主体的行为，数据主体的所在国之一应当设立代表。

4．为了确保对本条例的遵守，对于所有涉及到处理的事项，控制者或处理者应当做出强制性规定，确保其代表能在控制者或处理者之外收到信息，或者替代控制者或处理者收到信息，对于监管机构和数据主体所要求的事项尤其如此。

5．控制者或处理者委任代表，不能影响控制者或处理者进行的法律行动。

第 28 条 处理者

1．处理者代表控制者进行处理，控制者只能选用有充分保证的、可采取合适技术与组织措施的、其处理方式符合本条例要求并且保障数据主体权利的处理者。

2．如果没有控制者之前的特别授权或一般书面授权，处理者不应聘用另一个处理者。在具有一般书面授权的情形下，对于涉及到补充或替换其他处理者的变动，处理者都应当告知控制者，以便使控制者有机会反对此类变化。

3．处理者的处理应当受某类合同或其他欧盟法与成员国法的约束，这类合同或法律应当规定处理者相对于控制者的责任、主体事项、处理期限、处理性质与目的、个人数据的类型、数据主体的类型以及控制者的责任与权利的。此类合同或法律尤其应当对如下情形做出规定：

(a)只有在收到控制者的书面指示时才可以处理个人数据，在涉及到将个人数据转移到第三国或某个国际组织的事项中亦是如此，除非欧盟法或成员国法对处理者有要求；在这种情形下，处理者应当在处理之前将法律要求告知控制者，除非告知会影响重要的公共利益；

(b)对于被授权处理个人数据的人，确保其履行保密义务或法律上的适当保密责任；

(c)采取第 32 条所要求的所有措施；

(d)尊重第 2 段和第 4 段规定的聘用另一个处理者的条件；

(e)结合处理的性质，在可能的情形下，通过合适的技术与组织手段帮助控制者履行其责任，以便使得数据主体能够行使其第三章所规定的权利；

(f)结合处理的性质和处理者所能得到的信息，帮助控制者履行第 32 至 36 条所规定的责任；

(g)基于控制者的选择，在提供和处理相关的服务结束后，将个人数据删除或返还给控制者，并且删除已有备份，除非欧盟或成员国的法律要求储存个人数据；

(h)给控制者提供所有能够证明其已经遵循本条款规定责任的信息，以及有利于控制者或控制者委任的审计员进行审计和核查的信息。

关于第 1 段（h）点，如果处理者认为某项指示违反了本条例或其它欧盟或成员国的数据保护条款，其应当立即告知控制者。

4．当处理者代表控制者为了进行特定的处理活动而应聘另一处理者，第 3 段所规定的控制者和处理者之间的合同或其它法律条款所规定的数据保护责任应当通过合同或欧盟或成员国的法律条款而同等适用于另一处理者，尤其是应当采取充分的保障措施、恰当的技术与组织手段以满足本条例的要求。当另一个处理者无法完成其数据保护职责时，对其责任，处理者应当完全负担。

5．处理者遵守第 40 条所规定的已生效的行为准则，或者遵守第 42 条所规定的已生效的验证机制，这可以被作为证据之一，证明处理者已经采取了本条款第 1 段和第 4 段所规定的充分保障。

6．在不影响控制者和处理者之间的单独合同的前提下，第 3 段和第 4 段所规定的合同或法律条款可以全部或部分运用本条第 7 段和第 8 段所规定的格式合同条款，包括它们何时属于根据第 42 条和第 43 条规定的赋予给控制者或处理者的验证机制。

7．欧盟委员会可以对于本条第 3 段和第 4 段所规定的事项，根据第 93（2）条所规定的检查程序而制定格式合同条款。

8．监管机构可以对本条第 3 段和第 4 段所规定的事项，根据第 63 条所规定的一致性机制而制定格式合同条款。

9．第 3 段和第 4 段所规定的合同或法律条款必须是书面的，包括以电子形式做出的书面记录。

10．在不影响第 82、83、84 条的情形下，如果某个处理者因为确定处理目的与方法方而违反了本条例，处理者应当在此次处理中被视为控制者。

第 29 条 代表控制者或处理者进行的处理

对个人数据有访问权的处理者或控制者、处理者的代表人，未经控制者允许，不得处理该个人数据。欧盟法律或成员国法律另有规定的除外。

第 30 条 处理活动的记录

1．每个控制者——以及如果有的话——每个控制者的代表，都应当保持其所负责的处理活动的记录。这种记录应当包含所有如下信息：

(a)控制者以及——如果有的话——共同控制者、控制者的代表、数据保护官的姓名、详细联系方式；

(b)处理的目的；

(c)对数据主体的类型以及个人数据的类型的描述；

(d)个人数据已经被披露或将被披露给的接收者——包括位于第三国或国际组织的接收者——的类型；

(e)如果适用的话，将个人数据转移到第三国或国际组织的记录，包括识别此第三国或国际组织的记录，以及在第 49（1）条第二分段所提到转移的情形中，对适当保障措施的记录；

(f)如果适用的话，擦除不同种数据类型的预计期限；

(g)如果适用的话，对第 32（1）条所规定的技术性与组织性安全措施的一般性描述。

2．每个处理者以及——如果适用的话——处理者的代表对于以控制者名义进行的处理都应当保持保存一份记录，包含如下信息：

(a)处理者或处理者们的名字和详细联系方式、处理者所代表的每个控制者以及——如果有的话——控制者或处理者的代表、数据保护官；

(b)代表每个控制者进行处理的类型；

(c)如果适用的话，将个人数据转移到第三国或国际组织的记录，包括识别此第三国或国际组织的记录，以及在第 49（1）条第二分段所提到转移的情形中，对适当保障措施的记录；

(d)如果有的话，对第 32（1）条所规定的技术性和组织性安全措施的一般性描述。

3．第 1 段和第 2 段所规定的记录应当是书面的，包括以电子形式作出的书面记录。

4．基于监管机构的要求，控制者或处理者以及——在有的情况下——控制者或处理者的代表，应当提供可获取的记录。

5．第 1 和第 2 段所规定的责任不适用于雇员少于 250 人的经济主体或组织，除非其进行的处理不是偶尔性的，而且可能会对数据主体的权利与自由带来风险，或者其处理包含了第 9（1）条规定的特定种类的数据或第 10 条规定的和刑事犯罪和违法相关的个人数据。

第 31 条 和监管机构的合作

在监管机构的要求下，控制者和处理者以及——在适用的情况下——它们的代表应当配合监管机构的工作。

第二部分 个人数据的安全

第 32 条 处理的安全

1．在考虑了最新水平、实施成本、处理的性质、处理的范围、处理的语境与目的之后，以及处理给自然人权利与自由带来的伤害可能性与严重性之后，控制者和处理者应当采取包括但不限于如下的适当技术与组织措施，以便保证和风险相称的安全水平：

(a)个人数据的匿名化和加密；

(b)保持处理系统与服务的保密性、公正性、有效性以及重新恢复的能力；

(c)在遭受物理性或技术性事件的情形中，有能力恢复对个人数据的获取与访问；

(d)具有为保证处理安全而常规性地测试、评估与评价技术性与组织性手段有效性的流程。

2．在评估合适的安全级别的时候，应当特别考虑处理所带来的风险，特别是在个人数据传输、储存或处理过程中的的意外或非法销毁、丢失、篡改、未经授权的披露或访问。

3．遵守第 40 条所规定的已生效的行为准则，或者遵守第 42 条所规定的已生效的验证机制，这可以被作为证据之一，证明已经遵守了本条款第 1 段的要求。

4．控制者和处理者应当采取措施确保，除非接到控制者的指示，任何有权访问个人数据的处理者或任何代表控制者和处理者的自然人都不会进行处理，除非欧盟或成员国法律要求进行处理。

第 33 条 向监管机构报告对个人数据的泄露

1．在个人数据泄露的情形中，如果可行，控制者在知悉后应当及时——至迟在 72 小时内——将个人数据泄露告知第 55 条所规定的有权监管机构，除非个人数据泄露对于自然人的权利与自由不太可能会带来风险。对于不能在 72 小时以内告知监管机构的情形，应当提供延迟告知的原因。

2．处理者在获知个人数据泄露后，应当及时告知控制者。

3．第 1 段所规定的告知应当至少包括：

(a)描述个人数据泄露的性质，在可能的情形下，描述包括相关数据主体的类型和大致数量，以及涉及到个人数据的类型与大致数量；

(b)告知数据保护官的姓名与详细联系方式，或者可以获取更多信息的其他联系方式；

(c)描述个人数据泄露的可能后果；

(d)描述控制者应对个人数据泄露已经采用或计划采用的措施，包括——如果合适的话——减少负面影响的措施。

4．在不可能同时提供信息的情形下，可以分阶段地及时提供信息。

5．控制者应当记录所有对个人数据的泄露，包括泄露个人数据相关的事实、影响与已经采取的救济行动。参照该记录，监管机构得以核实控制者是否遵守本条例的有关规定。

第 34 条 向数据主体传达个人数据泄露

1．当个人数据泄露很可能给自然人的权利与自由带来高风险时，控制者应当及时向数据主体传达对个人数据泄露。

2．本条第 1 段所规定的向数据主体传达，应当以清晰和平白的语言传达个人数据泄露的性质，并且应当至少包括第 33（3）条（b）（c）（d）点所提供的信息与建议。

3．当满足如下情形之一时，不要求控制者告知数据主体其个人数据被泄露的信息：

(a)控制者已经采取合适的技术与组织保证措施，并且那些措施已经应用于那些被个人数据泄露所影响的个人数据，特别是已经应用那些使得未被授权访问的个人无法辨识个人数据的措施，例如加密；

(b)控制者已经采取后续措施，保证第 1 段所规定的给数据主体的权利与自由带来的高风险不再有实现的可能；

(c)告知将需要付出不相称的努力。此时，应存在公告机制或类似措施来承担控制者的告知义务，并且与控制者告知相比，这种措施的告知效果应当至少有相同效果。

4．如果控制者仍然没有将个人数据泄露告知数据主体，监管机构在考虑了个人数据泄露所可能带来的高风险可能性后，可以要求其告知，或者可以认为符合第 3 段所规定的情形。

第三部分 数据保护影响评估与提前咨询

第 35 条 数据保护影响评估

1．当某种类型的处理——特别是适用新技术进行的处理——很可能会对自然人的权利与自由带来高风险时，在考虑了处理的性质、范围、语境与目的后，控

制者应当在处理之前评估计划的处理进程对个人数据保护的影响。若多项高风险处理活动属于同一种类，那么此时仅对其中某一项活动进行评估即可。

2．如果控制者已经委任数据保护官，当其进行数据保护影响评估时，控制者应当向数据保护官进行咨询。

3．在如下情形中，第 1 段所规定的数据保护影响评估是尤其必须的：

(a)对与自然人相关的个人因素进行系统性与全面性的评价，此类评价建立在自动化处理——包括用户画像——基础上的，并且其决策对自然人产生法律影响或类似重大影响；

(b)以大规模处理的方式处理第 9（1）条所规定的特定类型的数据，或者和第 10 条规定的定罪与违法相关的个人数据；或者

(c)以大规模的方式系统性地监控某个公众可以访问的空间。

4．监管机构应当建立并公开一个列表，列明符合第 1 段所要求的数据保护影响评估的处理操作的类型。监管机构应当将此类列表告知第 68 条所提到欧盟数据保护委员会。

5．监管机构还可以建立一个公开性的列表，列明符合不需要进行数据保护影响评估的处理操作的类型。监管机构应当将此类列表告知欧盟数据保护委员会。

6．在设置第 4 段与第 5 段所规定的列表之前，当此类列表涉及到为数据主体提供商品或服务，或者涉及到对多个成员国行为的监管，或者可能实质性地影响欧盟内部个人数据的自由流动，有职权的监管机构应当首先适用第 63 条所规定的一致性机制。

7．评估应当至少包括：

(a)对计划的处理操作和处理目的的系统性描述，以及——如果适用的话——对控制者所追求的正当利益的描述；

(b)对和目的相关的处理操作的必要性与相称性进行分析；

(c)对第 1 段所规定的给数据主体的权利与自由带来的风险的评估；

(d)结合数据主体和其他相关个人的权利与正当利益，采取的计划性风险应对措施，包括保障个人数据保护和证明遵循本条例的安全保障、安全措施和机制。

8．评估相关控制者或处理者的处理操作的影响时，特别是评估数据保护影响时，应当合理考虑其对第 40 条所规定的已生效的行为准则的遵守。

9．在合适的情形下，如果其不影响保护商业或公共利益或处理操作的安全性，控制者应当咨询数据主体或数据主体代表对于其预期处理的观点。

10．当基于第 6（1）条（c）或（e）点而进行的处理符合欧盟或成员国为控制者制定涉及到处理操作的法律，并且在制定其法律基准时已经进行了作为一般性影响评估一部分的数据保护影响评估时，第 1 至 7 段不应当适用，除非成员国认为，有必要在处理活动前进行此类评估。

11．必要时，控制者应当进行核查，评估处理是否是符合数据保护影响评估，至少当处理操作所带来的风险存在变化时，应进行核查。

第 36 条 提前咨询

1．当第 35 条所规定的数据保护影响评估表明，如果控制者不采取措施，处理会带来高风险，那么控制者应当在处理之前咨询监管机构。

2．当监管机构认为，第 1 段所规定的预期的处理将违反本条例，特别是当控制者无法识别或减小风险，监管机构应当在收到咨询请求的八个星期以内向控制者以及——在适用的情况下——处理者提供书面建议，并且可以使用第 58 条所

规定的权力。考虑到预期处理的复杂性，这种期限可以延长六个星期。监管机构应当在收到咨询请求的一个月内向控制者以及——在适用的情况下——处理者告知延期以及延期的原因。监管机构可以延长期限，直到其获取了咨询所要求的信息。

3．当咨询第 1 段所规定的监管机构时，控制者应当向监管机构提供如下信息：

(a)在适用的情形下，涉及到处理——特别是当处理是在一群企业内部进行的——的控制者、共同控制者和处理者的相应责任；

(b)预期处理的目的与方法；

(c)为了保障数据主体权利与自由所采取的符合本条例的方法与措施；

(d)在适用的情形下，数据保护官的详细联系方式；

(e)第 35 条所规定的数据保护影响评估；以及

(f)监管机构要求的所有其它信息。

4．成员国在起草相关立法草案以获得国会通过时，或者根据此类立法措施制定处理相关的规制措施时，应当咨询监管机构。

5．虽然有第 1 段的规定，但在和控制者履行实现公共利益任务相关的处理中，包括和社会保障与公共健康相关的处理中，成员国法律可以要求控制者在其处理相关的事项中咨询监管机构并且提前获取监管机构的授权。

第四部分 数据保护官

第 37 条 数据保护官的委任

1．在如下任一情形中，控制者和处理者应当委任数据保护官：

(a)处理是公共机构或公共实体进行操作的，法庭在履行其司法职能时除外；

(b)控制者或处理者的核心处理活动天然性地需要大规模性地对数据主体进行常规和系统性的监控；或者

(c)控制者或处理者的核心活动包含了第 9 条规定的对某种特殊类型数据的大规模处理和第 10 条规定的对定罪和违法相关的个人数据的处理。

2．如果一组企业的每一个机构都能很容易联系数据保护官，这一组企业可以任命一个单独的数据保护官。

3．当控制者或处理者是一个公共机构或公共实体，基于它们的组织结构和规模，多个此类公共机构或实体可以共同委任一个数据保护官。

4．除了第 1 段所规定的情形，在欧盟或成员国法律要求的情形下，控制者或处理者，或代表某类控制者或处理者的协会和其他实体可以委任一名数据保护官。对于此类协会，或代表控制者或处理者的其他实体的活动，数据保护官有权代表它们进行活动。

5．数据保护官的委任必须基于其专业性的素质，其需要具有数据保护法律与实践的专业知识，以及完成第 39 条所规定的任务的能力。

6．数据保护官应当是控制者或处理者或基于服务合同而完成任务的一名职员。

7．控制者或处理者应当发布数据保护官的详细联系方式，并向监管机构进行报告。

第 38 条 数据保护官的职位

1．控制者和处理者应当确保，在所有与个人数据保护相关的事项中，数据保护官都应当以一种恰当和及时的方式介入。

2．控制者和处理者应当支持数据保护官履行第 39 条所规定的责任，应当提供其履行此类责任、访问个人数据、进行处理操作，以及维持其专业性知识的必要资源。

3．控制者和处理者应当确保个人数据保护官不会收到任何关于履行此类责任的指示。个人数据保护官不能因为完成其任务而被控制者或处理者解雇。其可以直接向控制者或处理者的最高管理层进行报告。

4．数据主体可以在所有和处理其个人数据相关的事项中，以及和行使本条例所赋予的权利相关的事项中联系数据保护官。

5．数据保护官在完成其任务时，应当遵守欧盟或成员国的法律，负有保密义务。

6．数据保护官可以完成其他任务或责任。控制者或处理者应当保证任何此类任务和责任不会导致利益冲突。

第 39 条 数据保护官的任务

1．数据保护官应当至少具有如下任务：

(a)对控制者或处理者，以及那些履行本条例和欧盟其他成员国数据保护条款所规定的处理责任的雇员进行告知，提供建议；

(b)确保遵守本条例、其他欧盟或成员国数据保护条款、和个人数据保护相关的控制者或处理者的政策，包括分配处理操作中以及相关审计中的责任、增强意识以及培训职员；

(c)根据要求，应当对数据保护影响评估以及根据第 35 条对其实施进行监管的事项提供建议；

(d)和监管机构进行合作；

(e)在与处理相关的事项中，包括第 36 条所规定的提前咨询中，以及——在适用的情况下——在其他所有相关事项的咨询中，充当监管机构的联系人。

2．数据保护官在履行其任务时，应当结合处理的性质、范围、语境与目的，合理地考虑处理操作所伴随的风险。

第五部分 行为准则与认证

第 40 条 行为准则

1．成员国、监管机构以及欧盟数据保护委员会与欧盟委员会鼓励在考虑不同处理部门的特征以及微型、小型以及中型经济主体的特定需求的基础上起草促进本条例合理适用的行为准则。

2．协会以及其它代表某类控制者或处理者的实体为了对适用本规则进行细化，可以起草行为准则，或修正或延长此类准则，例如，它们可以起草涉及到如下事项的准则：

(a)合理与透明的处理；

(b)在特定情境下控制者所追求的正当利益；

(c)对个人数据的收集；

(d)对个人数据进行匿名化处置；

(e)提供给公众与数据主体的信息；

(f)数据主体权利的行使；

(g)提供给儿童和保护儿童的信息，以及为了获取儿童监护人同意所采取的形式；

(h)第 24 条和第 25 条所规定的措施与程序，以及为了保障第 32 条所规定的处理安全所采取的措施；

(i)向监管机构通报个人数据泄露，以及将此类个人数据泄露告知数据主体；

(j)将个人数据转移到第三国或国际组织；或者

(k)不影响第 77 条和第 99 条所规定的数据主体权利的庭外诉讼性活动，以及为了解决控制者与数据主体在处理相关事项中争议的纠纷解决程序。

3．控制者或处理者除了受本条例约束之外，对于根据第 3 条不受本条例约束的情形，为了保证在第 46（2）条（e）点所规定的将个人数据转移到第三国或国际组织的框架中提供合适的安全措施，也可以受本条第 5 段所规定的已生效的行为准则约束，或者受本条第 9 段规定的具有一般性效力的行为准则所约束。为了提供此类合适的安全措施，包括和数据主体权利相关的安全措施，此类控制者或处理者应当通过合同或其他具有法律强制力的措施制定有约束力和可执行的承诺。

4．在不影响第 55 或 56 条所规定的有权监管机构的任务与权利的前提下，本条第 2 段所规定的行为准则应当包括使第 41（1）条所规定的实体能履行其监管任务的有效措施，保证负责实施行为准则的控制者或处理者遵循其条款的规定。

5．本条第 2 段所规定的计划起草、修改行为准则或延长现有准则的协会或其他实体，应当将准则草案、修正案或延期提议提交给符合第 55 条的有权监管机构。监管机构应当提供一份意见书，表明草案、修正案或延期提议是否符合本条例的规定，如果监管机构认定已经采取了足够和适当的安全保障，其应当批准草案、修正案或延期提议。

6．当准则草案、或修正案或延期提议是根据第 5 段的规定而被批准的，并且行为准则不涉及多个成员国的处理活动，监管机构应当进行登记并发表准则。

7．当行为准则的草案涉及到多个国家的处理活动，第 55 条所规定的有权监管机构应当在批准准则草案、修订或延期之前将其按照第 63 条规定的程序提交给欧盟数据保护委员会，并应提供一份意见书，表明准则草案、修正案或延期是否遵循了本条例，或者——在第 3 段所规定的情形中——是否提供了恰当的安全措施。

8．当第 7 段中规定的意见书确认了准则草案、修正案或延期遵循了本条例，或者——在第 3 段所规定的情形中——提供了恰当的安全措施，欧盟数据保护委员会应当将意见书提交给欧盟委员会。

9．欧盟委员会应当通过制定实施法案确定，根据第 8 段规定而提交的已生效的行为准则、修正案或延期是否在欧盟具有一般效力。此类法案的制定应当符合第 94（2）条所规定的核查程序。

10．对于已经被认定符合第 9 段中所规定的具有一般有效性的已生效准则，欧盟委员会应当保证其具有适当的公开性。

11．欧盟数据保护委员会应当核查所有登记的已生效行为准则、修正案以及延期，并且应当以恰当的方式使得公众能够获取。

第 41 条 对已生效行为准则的监控

1．在不影响第 57 和第 58 条规定的有权监管机构的任务与权利的前提下，对根据第 40 条制定的行为准则的合规性监管可以交给如下实体：在准则所规定事项方面具有适当的专业性，并且其合规性监管权力已经得到有权监管机构认证。

2．第 1 段所规定的实体，当存在如下条件时，可以被委任为有权监管是否遵守行为准则的机构：

(a)已经证明在准则所规定事项方面具有独立性与专业性，满足有权监管机构的要求；

(b)已经确立了相关程序，可以通过程序评估相关控制者和处理者适用准则的资质，监控其对准则条款的遵守，以及间歇性地评估其操作；

(c)已经设立程序和体系，解决关于违反准则，或关于控制者或处理者已经实施、或正在实施准则的方式的申诉，并且已使得此类程序与体系对数据主体和公众透明化；并且

(d)已经表明其符合有权监管机构的要求，其任务和职责不存在利益冲突的情形。

3．有权监管机构应当按照第 63 条所规定的一致性机制，将认证第 1 段中所规定的实体的标准草案提交给欧盟数据保护委员会。

4．当控制者或处理者违反准则，第 1 段所规定的实体在不影响有权监管机构的任务和权利、第八章条款的前提下，应当在适当安全措施的保障下采取合适的行动，包括准则中中止或剔除相关控制者或处理者。实体应当将此类行动以及行动的理由告知有权监管机构。

5．如果第 1 段所规定的实体不符合或不再符合认证的条件，或者其行为违反了本条例，有权监管机构应当撤回对其的认证。

6．本条不适用于公共机构和公共实体所进行的处理。

第 42 条 认证

1．成员国、监管机构、欧盟数据保护委员会和欧盟委员会应当鼓励——尤其是在欧盟层面——建立数据保护认证机制、数据保护印章和标记，以证明控制者

和处理者的处理操作符合本条例。对此应当考虑微型、小型以及中型经济主体的特定需求。

2．控制者或处理者除了受本条例约束之外，也可以设立符合本条第 5 段的数据保护认证机制、印章或标记，以便证明，对于根据第 3 条不受本条例约束的情形，已经对第 46（2）条（f）点所规定的将个人数据转移到第三国或国际组织的情形采取了合适的安全措施。为了提供此类合适的安全措施，包括和数据主体权利相关的安全措施，此类控制者或处理者应当通过合同或其他具有法律强制力的措施制定有约束力和可执行的承诺。

3．认证应当是自愿的，而且可以通过透明程序而获得。

4．根据本条而进行的认证，不能减轻控制者或处理者遵循本条例的责任，而且也不对第 55 条或 56 条所规定的有权监管机构的任务和权利产生影响。

5．符合本条的认证应当为第 43 条所规定的认证机构所批准，应当建立在第 58（3）条的有权监管机构或第 63 条的欧盟数据保护委员会所批准的标准之上。当标准被欧盟数据保护委员会所批准，这可以产生一个通用性认证——欧盟数据保护印章。

6．那些将其处理提交认证机制的控制者或处理者，应当将进行认证程序所必需的所有信息与访问权提交给第 43 条规定的认证机构，在适用的情形下，还应当提交给有权监管机构。

7．颁发给控制者或处理者的认证的有效期最长是三年，如果相关条件满足，同样的情形下有效期可以延长。当认证的条件不满足或不再满足时，在适用的情形下，第 43 条规定的认证实体或有权监管机构可以撤回认证。

8．欧盟数据保护委员会应当核查所有已登记的验证机制、数据保护印章和标记，而且应当以恰当的方式使得公众能够获取。

第 43 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与权利的前提下，具有相应专业性的认证机构可以在告知监管机构后——以便监管机构可以行使第 58（2）点 h 点所规定的权利——颁发和更新认证。成员国应当确保这些认证机构是如下一个机构认可或两个机构同时认可的：

(a)第 55 或 56 条所规定的有权监管机构；

(b)按照欧洲议会和理事会的(EC)No 765/2008 条例、EN-ISO/IEC 17065/2012 设定的，以及满足第 55 条或第 56 条的有权监管机构所规定的额外要求的全国性认证机构。

2．只有存在如下情形时，第 1 段所规定的认证机构才能根据第 1 段的规定被认证：

(a)已经证明在准则所规定事项方面具有独立性与专业性，满足有权监管机构的要求；

(b)采取措施遵从第 42（5）条所规定的标准，并且已经为第 55 条所规定的有权监管机构或第 63 条规定的欧盟数据保护委员会所批准；

(c)建立了发行、定期审查和撤回数据保护认证、印章和标记的程序；

(d)已经设立了解决关于违反准则，或关于控制者或处理者已经实施、或正在实施准则的方式的申诉程序和体系，并且数据主体和公众已知悉此类程序和体系；且

(e)已经表明其符合有权监管机构的要求，其任务和职责不存在利益冲突的情形。

3．第 1 段和第 2 段所规定的委任认证机构应当建立在第 55 条或第 66 条所规定的有权监管机构所批准的基础性标准之上，或者第 63 条所规定的欧盟数据保护委员会所批准的基础性标准之上。对于本条第 1 段（b）点所规定的授权，此类要求应当补充(EC) No 765/2008 指令所设想的要求，以及描述认证机构方法与程序的技术性规则。

4．在不影响控制者或处理者对本条例的遵守的前提下，第 1 段所规定的认证机构应当负责颁发认证或撤销此类认证的有效评估。颁发给控制者或处理者的认证的有效期最长是五年，如果相关条件满足，同样的情形下有效期可以延长。

5．第 1 段所规定的验证机构应当向有权监管机构报告颁发或撤销所要求认证的理由。

6．监管机构应当以容易获取的方式公开本条第 3 段所规定的要求，以及第 42（5）段所规定的标准。监管机构还应当将那些要求和标准传输给欧盟数据保护委员会。欧盟数据保护委员会应当核查所有登记的认证机制与数据保护印章，而且应当通过某种恰当的方式将它们公开。

7．在不影响第八章的前提下，当认证的条件不符合或不再符合，或者当认证机构所采取的行为侵犯了本条例，有权监管机构或全国性的认证机构应当取消根据本条第 1 段对认证机构的认证。

8．为了细化第 42（1）条所规定的数据保护验证机制所需要考虑的条件，欧盟委员会有权制定符合第 92 条的授权法案。

9．欧盟委员会可以制定实施法案，为验证机制与数据保护印章、标记与机制设定技术标准，以便促进和认可那些验证机制、印章与标记。此类实施法条的制定应当符合第 94（2）条所规定的验证程序。

第五章 将个人数据转移到第三国或国际组织

第 44 条 转移的一般性原则

对于正在处理或计划进行处理的个人数据，将其转移到第三国或国际组织，包括将个人数据从第三国或国际组织转移到另一第三国或另一国际组织，控制者和处理者只有满足本条例的其他条款，以及满足本章规定的条件才能进行转移。为了保证本条例对于自然人的保护程度不会被削弱，本章的所有条款都应当被遵守。

第 45 条 基于认定具有充足保护的转移

1．当欧盟委员会作出认定，认为相关的第三国、第三国中的某区域或一个或多个特定部门、或国际组织具有充足保护，可以将个人数据转移到第三国或国际组织。此类转移不需要特定的授权。

2．当评估保护程度的充足性时，欧盟委员会应当特别考虑如下因素：

(a)法治、对人权与基本自由的尊重、包括关于公共安全、国防、国家安全、刑法和公共机构访问个人数据的一般性与部门性立法，以及此类立法的实施、数据保护规则、职业规则和安全措施，包括将个人数据转移到另一第三国或国际组织所必须遵循的第三国或国际组织的规则、判例法以及有效可执行的数据主体权利、对其个人数据正在转移的数据主体的司法救济；

(b)在国际组织是主体的情形中，第三国内存在一个或多个有效运作的独立监管机构，保证数据保护规则的实施，包括具有充分的执行权力，在数据主体行使其权利时和与成员国的监管机构合作时提供帮助和建议；

(c)第三国或国际组织已经许下的国际性承诺，或者承诺愿意承担有法律约束力的条约或法律文件所引起的其它责任，以及参加多边或地区性的体系，特别是和数据保护相关的体系所引起的其它责任。

3．在评估了保护程度的充足性之后，欧盟委员会可以通过制定实施性法案，确定本条第 2 段含义内的第三国、第三国内的领地或一个或多个特定部门或一个国际组织是否具有充足的保护。实施性法案应当提供一种周期性审查，至少每四年对第三国或国际组织的所有相关发展进行审查。实施性法案应当细化其领域性与部门性的实施，以及在适用的情况下确定本条第 2 段（b）点所规定的一个或多个监管机构。实施性法案的制定应当遵循第 93（2）条所规定的验证程序。

4．欧盟委员会应当持续性地监控第三国或国际组织的某些可能会影响根据本条第 3 款而作出的决定和建立在 95/46/EC 指令第 25（6）条基础之上的决定发挥作用的某些发展。

5．当已有信息显示，第三国或第三国内的一个或多个特殊部门或国际组织不再提供本条第 2 段所规定的充足的保护，欧盟委员会应当——尤其是在经过第 3 段所规定的核查后——通过制定不具有溯及力的实施性法案，在必要限度内废止、修正或中止本条第 3 段所规定的决定。此类实施性法案的制定应当遵循第 93（2）条所规定的验证程序。

在具有高度正当性的紧急状态情形中，欧盟委员会应当立即根据第 93（3）条规定的程序而制定实施性法案。

6．为了补救导致第 5 条决定的情形，欧盟委员会应当与第三国或国际组织磋商。

7．符合本条第 5 段的决定不会影响到将个人数据转移到第三国、第三国内的领地或一个或多个部门、或者第 46 条至 49 条所规定的相关国际组织。

8．欧盟委员会应当在欧盟的官方杂志及其网站上发表名单，列明其确定已经具备充足保护或不再具有充足保护的第三国、第三国内的特定部门和国际组织。

9．欧盟委员会在 95/46/EC 指令第 25（6）条基础上而做出的决定，在被欧盟委员会根据本条第 3 段或第 5 段而修改、替代或废止前应具有效力。

第 46 条 转移所需要的适当安全保障

1．如果没有根据第 45（3）条而做出的决定，控制者或处理者只有提供适当的保障措施，以及为数据主体提供可执行的权利与有效的法律救济措施，才能将个人数据转移到第三国或一个国际组织。

2．在不要求监管机构提供任何具体授权的情形下，第 1 段所规定的适当保障措施可以如下方式提供：

(a)公共机构或实体之间之间签订的具有法律约束力和可执行性的文件；

(b)符合第 47 条的有约束力的公司规则；

(c)欧盟委员会根据第 93（2）条规定的核查程序而制定的数据保护标准条款；

(d)监管机构根据第 93（2）条规定的核查程序制定并且为欧盟委员会批准的数据保护标准条款；

(e)根据第 40 条制定的行为准则，以及第三国的控制者或处理者为了采取合适的安全保障而做出的具有约束力和执行力的承诺，包括数据主体的权利；或者

(f)根据第 42 条而被批准的验证机制，以及第三国的控制者或处理者为了采取合适的安全保障而做出的具有约束力和执行力的承诺，包括数据主体的权利。

3．在需要有权监管机构授权的情形下，第 1 段所规定的合适安全措施尤其可以通过如下方式进行规定：

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

(b)公共机构或公共实体之间在行政性安排中所插入的条款，包括可执行的与有效的数据主体权利。

4．在本条第 3 段所规定的情形中，监管机构应当适用第 63 段所规定的一致性机制。

5．成员国或监管机构根据 95/46/EC 指令的第 26（2）条而做出的授权，在被监管机构修改、替代或废止之前应当一直有效。欧盟委员会根据 95/46/EC 指令第 26（4）条而做出的决定，在欧盟委员会按照本条第 2 段做出必要性的修改、替换或废止决定前应当一直有效。

第 47 条 有约束力的公司规则

1．在满足如下条件时，对于符合第 63 条所规定的一致性机制的有约束力的公司规则，有权监管机关应当批准：

(a)具有法律约束力，适用于进行联合经济活动的企业集团或一系列经济主体的所有相关成员——包括其雇员，并且为他们所执行。

(b)在处理个人数据方面明确赋予数据主体以可执行的权利；以及

(c)满足第 2 段所规定的要求。

2．第 1 段所规定的有约束力的规则应当至少明确：

(a)进行联合经济活动的企业集团或一系列经济主体，及其每一个成员的架构和详细联系方式；

(b)数据转移或一系列的数据转移，包括个人数据的类型；处理类型及其目的；受影响的数据主体的类型；以及涉及到的对第三国或多个第三国的确定；

(c)规则的法律约束效力，既包括内部的约束力，也包括外部的约束力；

(d)对一般数据保护原则的适用，特别是目的限定、数据最小化、有限的储存期限、数据质量、通过设计的数据保护与默认的数据保护、处理的法律基础、对特定类型个人数据的处理；保障数据安全的措施；以及将数据转移到不受约束性公司规则所约束的实体所做的要求；

(e)和处理相关的数据主体的权利以及行使这些权利的方式，包括有权不被仅仅根据自动化处理——包括符合第 22 条的用户画像——而对数据主体做出决定，有权按照第 79 条向有权监管机构和成员国的有权管辖的法庭申诉，以及有权在违反有约束力的公司规则的情形下获取救济和——如果适用的话——赔偿；

(f)对于任何不在欧盟设立的控制者或处理者的相关成员违反约束性公司规则，在成员国的领域内设立的控制者或处理者愿意承担责任；只有当控制者或处理者证明，该成员对于导致损害的事件没有责任，控制者或处理者的此种责任才能被免除；

(g)关于约束性公司规则的信息如何提供给数据主体，特别是第 13 和 14 条之外关于本段所规定的(d)(e)(f)点的信息如何提供给数据主体；

(h)根据第 37 条所委任的所有数据保护官的任务，或者企业集团、或进行联合经济活动的一系列经济主体内部负责监控遵守约束性公司规则、监控培训和处置申诉的所有人或实体的任务；

(i)申诉程序；

(j)企业集团或进行联合经济活动的一系列经济主体，为了核实对约束性公司规则的遵守的而在内部所设立机制。此类机制应当包括数据保护核查以及能够确保采取矫正性活动保护数据主体权利的方法。此类核实结果应当告知（h）点所规定的个人或实体，企业集团或进行联合经济活动的一系列经济主体，而且在有权监管机构的要求下应当能够提供其核实结果；

(k)报告和记录规则变化的机制，以及将此类变化报告给监管机构的机制；

(l)为了保证企业集团或进行联合经济活动的一系列经济主体的合规性而和监管机构一起设立的合作机制，特别是向监管机构提供（j）点所规定的方法的核查结果；

(m)企业集团或进行联合经济活动的一系列经济主体的成员是第三国的主体，可能会对约束性企业规则所提供的保障产生实质性的负面影响，向有权监管机构报告对此类主体是否有法律要求的机制；以及

(n)对于可永久性或经常性访问个人数据的员工进行的适当数据保护培训。

3．欧盟委员会可以明确控制者、处理者和监管机构之间为了本条含义内的约束性公司规则而进行信息交换的形式和程序。此类实施性法案的制定应当遵循第 93（2）条所规定的验证程序。

第 48 条 未经欧盟法授权的转移或披露

任何法庭判决、仲裁裁决或第三国行政机构的决定，若要求控制者或处理者对个人数据进行转移或披露，同时满足以下条件时方能得到认可或执行：一是该判决、裁决或决定必须基于提出请求的第三国与欧盟或其成员国之间订立的法律互助协议等国际条约，二是该判决、裁决或决定不会对本章规定的其他转移形式产生消极影响。

第 49 条 特殊情形下的克减

1．如果不存在根据第 45（3）而做出的充足保护认定或根据第 46 条而制定的适当安全措施——包括约束性公司规则，将个人数据转移到第三国或国际机构，只有满足如下情形之一才能进行：

(a)数据主体被明确告知，不存在充足保护或适当的安全措施，预期的数据转移存在风险，但之后数据主体仍然明确表示同意预期的数据转移；

(b)转移对于履行数据主体与控制者之间的合同，或者履行数据主体在签订契约前所提出要求是必要的；

(c)控制者和另一自然人或法人之间签订或履行合同时，转移对于实现数据主体的利益是必要的；

(d)转移对于实现公共利益是必要的；

(e)转移对于确立、行使或辩护法律性主张是必要的；

(f)当数据主体基于身体性或法律性原因无法表达同意，为了保护数据主体或其他人的关键利益是必要的；

(g)转移是根据登记册而进行的——这种登记册是欧盟法或成员国法律为了向具有正当利益的一般性公众或个人提供咨询。但是，只有满足欧盟法或成员国法对咨询所规定必要条件，此类个案中的转移才能进行克减。

当转移无法基于第 45 或第 46 条，包括基于约束性公司规则的条款的规定而进行，且从（a）点到（g）的克减条件都不符合，将数据转移到第三国或国际组织，这只有在转移满足如下条件时才可以：转移是非重复性的；关乎很小一部分数据主体的权利；对于实现控制者压倒性的正当利益是必要的，并且不会违反数据主体的有限性的利益或权利与自由；控制者已经对围绕数据传输的情形进行评估，而且基于这种评估对个人数据保护采取了合适的安全保障。控制者除了提供第 13 条和第 14 条所规定的信息之外，应当将转移和追求的压倒性正当利益告知数据主体。

2．符合第 1 段（g）点的转移不应当包括登记册里的全部个人数据或所有类型的个人数据。当登记册是为了给具有正当利益的人提供咨询的，只有那些人提出要求，或者那些人是接收者的情形才能进行转移。

3．对于公共机构在行使其公共权力时的活动，第 1 段的（a）（b）（c）点以及第 1 段的第二分段不适用。

4．第 1 段（d）点规定的公共利益应当为欧盟或成员国为控制者所制定的法律所确认。

5．如果不存在充足保护的认定，欧盟或成员国的法律可以基于公共利益而明确做出限制，限制将个人数据转移到第三国或国际组织的特定类型。成员国应当将此类条款告知欧盟委员会。

6．控制者或处理者应当在第 30 条规定的档案中记录本条第 1 段第二分段所规定的评估以及合适的安全措施。

第 50 条　为保护个人数据的国际合作

在涉及到第三国或国际组织的情形中，欧盟委员会和监管机构应当采取合适的措施以：

(a)发展国际合作机制，以便促进对个人数据保护立法的有效实施；

(b)在采取合适安全措施保障个人数据保护和其它基本权利与自由的前提下，通过告知、申诉转介、调查帮助和信息互换为个人数据保护立法的实施提供国际性互助；

(c)在实施个人数据保护立法中，使相关利益方密切参与为了进一步国际合作而进行的讨论和活动；

(d)促进个人数据立法与实践——包括与第三国管辖权冲突——的交换与记录。

第六章 独立监管机构

第一部分 独立性地位

第 51 条 监管机构

1．为了保护自然人在处理过程中的基本权利与自由，以及促进欧盟内部的个人数据的自由流通，每个成员国应当建立一个或多个独立公共机构，负责监控本条例的实施。

2．每个监管机构都应当帮助本条例在欧盟的一致性适用。基于这种目的，监管机构应当按照第七章的规定彼此合作以及和欧盟委员会合作。

3．当一个成员国确立了不止一个监管机构，该成员国应当在欧盟数据保护委员会委任一个监管机构代表其他机构，而且应当建立一套机制，保证其他机构遵守第 63 条规定的一致性机制相关的规则。

4．每个成员国都应当将其根据本章所制定的法律条款告知欧盟委员会，[最迟应当在本条例生效的两年内]，而且应当及时将影响条款的修订告知欧盟委员会。

第 52 条 独立性

1．每个监管机构在行使其任务和行使符合本条例的权力时，应当保持完全的独立性。

2．每个监管机构的一个或多个成员在行使其任务和行使符合本条例的权力时，应当不受外部影响，不论是直接的还是间接性的，而且不应接收任何人的指示。

3．监管机构的成员不得从事违反其监管职责的活动，任职期间不得担任任何与其监管工作相冲突的有偿或无偿的职务。

4．每个成员国都必须确保，每个监管机构都具有为了有效履行其任务和行使其权利——包括在欧盟数据保护委员会中互助、合作和参与的履行任务和行使权利——所必需的人力性、技术性与资金资源，前提性与基础性要素。

5．每个成员国都应当确保，每个监管机构都具有选择和雇佣其成员的权力，这只受相关监管机构的一个或多个成员的专门指令的约束。

6．每个成员国都必须确保，在不影响其独立性以及其具有单独和公共性的年度预算的前提下，每个监管机构都受资金控制——此类资金控制可能是州预算或国家预算一部分的——的约束。

第 53 条 监管机构成员的一般性要求

1．成员国应当通过如下机构以透明化的方式委任其监管机构的每个成员：

-它们的议会；

-它们的政府；

-它们的国家元首；或者

-成员国法律指派的独立性实体。

2．每个成员都应当具有履行其职责和行使其权力所应当具有的资质、经验与技巧，特别是在个人数据保护领域的资质、经验与技巧。

3．成员根据成员国的相关法律结束其任期、辞职或强制性退休时，其职责也相应结束。

4．只有存在严重的不当行为，或者不再符合履行其职责的条件时，成员才可以被解职。

第 54 条 设立监管机构的规则

1．每个成员国都应当通过法律规定如下事项：

(a)每个监管机构的设立；

(b)被任命为每个监管机构的成员所需要的资质与合适的条件；

(c)任命每个监管机构的一个或多个成员的规则和程序；

(d)每个监管机构的一个或多个成员的不少于四年的任期，（在此条例生效之后的第一次任命例外），如果有必要通过间断性的任命程序来保护监管机构的独立性，一部分成员的任期可以更短；

(e)每个监管机构的一个或多个成员是否可以连任，如果可以的话，可以连任多少个任期；

(f)每个监管机构的成员和员工需要负责的情形，对于其任期内或任期结束后的具有冲突性的行为、任职和收益的禁止条款，以及中止雇佣的规则。

2．每个监管机构的成员和员工都应当遵循欧盟或成员国的法律，对于其履行任务或行使其权力期间所获取的秘密信息，在任职期间或任期结束后都具有保守职业秘密的职责。尤其在自然人报告具有违反本条例的情形下，成员或员工应当履行其保守职业秘密的职责。

第二部分 职权、任务与权力

第 55 条 职权

1．每个监管机构都有权在其所属的成员国境内根据本条例履行分配给其的任务，行使授予其的权力。

2．当公共机构或私人实体基于第 6（1）条的（c）或（e）点而进行处理，成员国的相关监管机构应当拥有职权。在此类情形中，第 56 条不适用。

3．对于法庭在其司法活动中进行处理操作，监管机构不具有监管职权。

第 56 条 领导性监管机构的职权

1．在不影响第 55 条的前提下，控制者或处理者的主要营业机构或唯一营业机构所在地的监管机构应可以充当领导性监管机构，监管控制者或处理者根据第 60 条程序而进行的跨境处理。

2．第 1 段的规定可以进行减免，如果主要事项只和成员国内的一个机构相关，或者只在一个成员国内对数据主体产生实质性影响，每个监管机构应当都有权对向其进行的申诉或违反本条例的行为进行处置。

3．对于第 2 段所规定的情形，监管机构应当将此事项及时告知领导性监管机构。在被告知的三个星期以内，领导性的监管机构应当——结合控制者或处理者是否在通知其的监管机构所在的成员国内有拥有机构——决定，其是否要根据第 60 条的规定的程序而处置该案例。

4．当领导性监管机构决定处理案件，第 60 条所规定的程序应当适用。那个告知领导性监管机构的监管机构可以向领导性监管机构提交一份决定草案。当领导性监管机构起草第 60（3）条所规定的决定时，其应当尽最大限度地考虑提交的决定草案。

5．当领导性监管机构决定不处置案子，通知领导性监管机构的监管机构应当根据第 61 条和第 62 条进行处置。

6．对于控制者或处理者所进行的跨境处理，领导性监管机构应当是该控制者或处理者的唯一面谈者。

第 57 条 任务

1．在不影响本条例规定的其他任务的前提下，在其管辖范围内，每个监管机构应当：

(a)监控和执行对本条例的实施；

(b)提高公众意识，对和处理相关的风险、规则、安全保障和权利的理解。对针对儿童的活动保持特别注意；

(c)根据成员国的法律、全国性议会、政府以及其他制度和实体对与处理相关的自然人的权利与自由提供建议；

(d)提高控制者与处理者对本条例所规定责任的意识；

(e) 基于要求为所有数据主体提供行使本条例所规定的权利，以及——如果适用的话——和其它成员国的监管机构为了实现这一目的而进行合作；

(f)处置数据主体或实体、组织或协会根据第 80 条的申诉，采用合适的手段调查申诉的主要事项，在合理期限内向申诉者告知进展和调查结论——特别是如果需要进一步的调查或和监管机构协调；

(g)为保证对本条例适用与执行的一致性和其他监管机构合作，包括分享信息和提供相互协助；

(h)为本条例的适用进行调查，包括基于另一监管机构或其它公共机构提供的信息而进行的调查；

(i)在相关发展——特别是信息和通讯技术、商业实践发展——对个人数据保护产生影响的情况下，对相关发展进行监控；

(j)采用第 28（8）条和第 46（2）条（d）点规定的标准格式合同；

(k)建立并维持和第 35（4）条规定的个人数据保护影响评估相关的条目；

(l)对第 36（2）条规定的处理操作给出建议；

(m)鼓励起草符合第 40 条的行为准则，对符合第 40（5）条提供充分安全保障的此类行为准则提供意见并进行批准；

(n)鼓励设立数据保护认证机制以及符合第 42（1）条的数据保护印章与标记，并批准符合第 42（5）条的认证标准；

(o)在适用的情形下，对根据第 42（7）条而颁发的认证进行阶段性审查；

(p)对符合第 41 条规定的监控行为准则的委派实体，以及符合第 43 条规定的认证实体，对其标准进行起草并发布；

(q)委任符合第 41 条规定的监控行为准则的实体，以及符合第 43 条规定的认证实体；

(r)授权合同条款与第 46（3）条规定的条款；

(s)批准符合第 47 条的约束性合同规则；

(t)欧盟数据保护委员会的活动提供帮助；

(u)对违反本条例的情形以及根据第 58（2）条而采取的措施保持内部纪录；并且

(v)完成和个人数据保护相关的其它任务。

2．每个监管机构都应当为第 1 段（f）点规定的提交申诉提供便利，例如在不排除其它通讯方式的前提下，提供可以通过电子方式填写和提交的申诉方式。

3．每个监管机构的任务履行对于数据主体都应当是免费的，如果适用的话，对于数据保护官也应当是免费的。

4．当请求是明显毫无根据的或过分的，特别是当请求是重复性的，监管可以基于行政花费而收取一定的合理费用，或拒绝对请求作出行动。监管机构有责任证明，请求是明显毫无根据的或过分的。

第 58 条 权力

1．每个监管机构都具有所有如下调查权力：

(a)要求控制者和处理者，以及——在适合的情形下——控制者或处理者的代表提供履行其任务所需要的所有信息；

(b)以数据保护核查的方式进行调查；

(c)对根据第 42（7）所颁布的认证进行审查；

(d)将可能侵犯本条例的情况告知控制者或处理者；

(e)从控制者或处理者那里获取访问个人数据的权力，以及为了行使其任务而所需的所有信息；

(f)按照欧盟与成员国法律的程序法，获取对控制者和处理者的所有房屋建筑及场地，包括数据处理设施和方法的访问权。

2．每个监管机构都有所有如下矫正性权力：

(a)对控制者或处理者颁发警告，警告预期的处理操作可能会侵犯本条例的条款；

(b)当处理操作侵犯本条例条款的时候，对控制者或处理者进行申诫；

(c)命令控制者或处理者尊重数据主体行使符合本条例的权利；

(d)命令控制者或处理者的处理操作符合本条例条款，如果适合的话，应当在特定的期限内以特定的方式完成；

(e)命令控制者将个人数据泄露的情况告知数据主体；

(f)对处理施加暂时性或具有明确期限的禁令；

(g)要求对个人数据进行纠正或擦除，或根据第 16 条，17 条和 18 条而对处理进行限制，以及将此类行动告知第 17（2）条和第 19 条规定的个人数据披露给的接收者；

(h)撤回认证，或命令认证机构撤回根据第 42 条和第 43 条而颁发的认证，或者当认证的要求不满足或不再满足时，命令认证机构不要颁发认证；

(i)视每个案例的情形不同，在本段所规定的措施之外，或者替代本段所规定的措施而采取第 83 条规定的行政处罚；

(j)要求中止将数据传输到第三国或国际组织。

3．每个监管机构都有所有如下授权和建议的权力：

(a)根据第 36 条规定的提前咨询条款向控制者提出建议；

(b)主动或根据要求为全国性议会、成员国政府提供意见，或者根据成员国法为其他机构、实体与公众提供和个人数据保护相关的保护；

(c)如果成员国的法律要求此类提前咨询，根据第 36（5）条而授权处理；

(d)根据第 40（5）条而发布意见以及行为准则；

(e)根据第 43 条而委任认证机构；

(f)根据第 42（5）条颁发认证和批准认证的标准；

(g)制定第 28（8）条以及第 46（2）条（d）点规定的数据保护标准条款；

(h)授权第 46（3）条（a）点规定的合同条款；

(i)授权第 46（3）条（b）点规定的行政性安排；

(j)批准符合第 47 条的约束性公司规则。

4．根据本条而行使赋予给监管机构的权力应当满足合适的安全保障，包括根据欧盟宪章而在欧盟和成员国法律中规定的有效司法救济和正当程序。

5．每个成员国应当通过法律规定，其监管机构为了执行本条例的条款，有权将违反本条例的情形诉诸司法机构，在合适的情形下可以提起或参与法律诉讼。

6．每个成员国都应当通过法律规定，其监管机构具有第 1、2 和 3 段规定的附加权力。对那些权利的行使不应当削弱第七章规定的有效运行。

第 59 条 活动报告

每个监管机构都应当起草一份关于其活动的年度报告，这可以包括其被告知的违法类型以及根据第 58（2）条而采取的措施类型。此类报告应当传输给全国性议会、政府以及成员国法律所委任的其他机构。公众、欧盟委员会和欧盟数据保护委员会应当能够获取这些报告。

第七章 合作与一致性

第一部分 合作

第 60 条 领导性监管机构和其他相关监管机构的合作

1．领导性监管机构应当根据本条和其他相关监管机构进行合作，努力达成共识。领导性监管机构和相关监管机构应当彼此分享相关信息。

2．领导性监管机构可以随时要求其他相关监管机构提供第 61 条规定的互助合作，而且可以根据第 62 条而进行联合行动，这尤其适用于如下情形：为了进行调查，或者为了实施涉及到设立在另一成员国的控制者或处理者的措施。

3．领导性监管机构应当及时将事项相关信息告知给其他相关监管机构。对于其他相关监管机构的意见，其应当充分考虑，并及时向其他相关监管机构提交一份决定草案。

4．当其他任何相关监管机构收到第 3 段中所规定的咨询，并在四周内表达了对决定草案的相关与合理的反对，领导性监管机构如果不同意此相关与合理的反对，或者认为其意见是不相关或不合理的，应当将此事项提交给第 63 条规定的一致性机制。

5．如果领导性的监管机构同意相关与合理的反对意见，对于此反对意见，其应当将一份修订后的草案决定提交给其他监管机构。修订后的草案决定应当遵守第 4 段所规定的程序，并且应当在两个星期内做出。

6．如果在第 4 段和第 5 段所规定的期间内，其他相关监管机构都没有反对领导性监管机构所提交的决定草案，应当推定领导性的监管机构和相关监管机构对于决定草案具有一致意见，而且应当受其约束。

7．领导性监管机构应当做出决定，将决定的情况——包括相关事实和理由的总结——通知给控制者或处理者的主要营业机构或唯一营业机构，并视情况通过其他相关监管机构以及做出该决定的欧盟数据保护委员会。收到申诉的监管机构应当将决定的情况告知给申诉者。

8．在申诉被撤销或驳回的情形中，第 7 段的规定可以进行克减，收到申诉的监管机构应当采用决定并将其告知申诉者，由此也告知了控制者。

9．当领导性监管机构和相关监管机构同意撤销或驳回申诉的一部分，对申诉的其他部分采取行动，对于此类其他部分的事项，应当采取单独的决定。领导性监管机构应当采用和控制者行动相关的那部分决定，将其通告给控制者或处理者在成员国境内的主要营业机构或唯一营业机构，由此也告知了申诉者。另一方面，申诉者的监管机构应当采用和撤销或驳回申诉相关的那部分决定，将其告知申诉者，由此也告知了控制者或处理者。

10．当收到领导性监管机构根据第 7 段和第 9 段而进行的告知后，控制者或处理者应当采取必要措施，保证其在欧盟所有的所有机构的处理活动都符合决定。控制者或处理者应当向领导性监管机构告知为遵守决定而采取的措施，并通知其他相关监管机构。

11．在极端情形下，当某相关监管机构认为，有充分理由证明需要采取紧急行动以保护数据主体的利益，应当援引第 66 条有关紧急程序的规定。

12．领导性监管机构和其他相关监管机构应当通过电子方式，以标准化的格式为彼此提供本条所要求提供的信息。

第 61 条　互相协助

1．监管机构应当为彼此提供信息和互相协助，以便以一种一致性的方式执行和适用本条例，而且应当拥有有效信息以进行有效的相互合作。互相协助尤其应当包括信息请求和监管措施，例如在授权与咨询、检验与调查之前请求信息和采取监管措施。

2．对于另一监管机构的请求，每个监管机构都应当采取恰当的合适措施及时回应，而且至迟应当在收到请求内的一个月内进行。此类措施尤其可以包括传输和调查相关的信息。

3．请求协助应当包括所有必要信息，包括请求的目的与原因。被交换的信息只能被用于实现请求协助的目的。

4．除非存在如下情形，被请求的监管机构不应当拒绝请求：

(a)被请求的监管机构对被请求的主体事项或被请求执行的措施没有职权；或者

(b)被请求的监管机构对请求进行照办，这会侵犯本条例或欧盟或成员国的为被请求的监管机构所制定的法律。

5．被请求的监管机构应将结果告知发出请求的监管机构，而且应当视情况告知为了实现请求而采取的措施。被请求的监管机构如果拒绝按第 4 段而提出的请求，应当提供说明。

6．基于其他监管机构的请求，被请求的监管机构应当以电子形式，使用标准化的格式提供信息，这应当成为一项规则。

7．所有被请求的监管机构根据请求而进行的互相协作，都不应当收取费用。对于特定情形下因为提供互相协作而产生的特定花费，监管机构之间可以签订补偿规则。

8．当某监管机构在收到另一监管的请求后一个月内仍然不提供第 5 段所规定的信息，做出请求的监管机构可以根据第 55（1）条在其成员国境内采取临时性措施。在这种情形中，可以推定为符合第 66（1）条的紧急情况，欧盟数据保护委员会应根据第 66（1）条而作出紧急约束性决定。

9．欧盟数据保护委员会可以通过制定实施性法案而细化本条规定的互相协助的形式与程序，在监管机构之间、监管机构和欧盟委员会之间以电子方式进行的信息交换，特别是本条第 6 段所规定的标准化格式。此类实施性法案的制定应当遵循第 93（2）条规定的验证程序。

第 62 条 监管机构的联合行动

1．在合适的时候，监管机构应当进行联合行动，包括在涉及到其他成员国监管机构的成员或员工的情形下进行联合调查和采取联合执行措施。

2．当控制者或处理者在多个成员国设立机构，或者当两国或两国以上的数据主体可能会受处理操作的实质性影响，这些成员国的监管机构都有权参与联合行动。按照第 56（1）或 56（4）条规定而拥有职权的监管机构可以邀请这些成员国中的每个国家的监管机构参与联合行动，而且应当及时回应某监管机构的参与请求。

3．一个监管机构可以按照成员国的法律，以及临时调派的监管机构的授权，将调查权等权力授权给临时调查的监管机构的成员或员工。或者，如果监管机构的成员国的法律允许，应当允许临时调派的监管机构的成员或员工行使其符合成员国法律对其做出规定的调查权。只有在东道主监管机构的成员或员工的指导和见证之下，此类权力才能被行使。临时调派的监管机构的成员或员工应当遵守东道主监管机构所在的成员国国家的法律。

4．当根据第一段的规定临时调派的监管机构在另一成员国内活动，东道主监管机构所在的成员国应当对其行动承担责任，包括对活动期间所引起的损害，应当按照其活动地所属的成员国法律承担责任。

5．对于成员国境内所造成的损害，如果其可以适用其成员国的损害赔偿，成员国应当进行赔偿。临时调派的监管机构的某成员国的员工对另一成员国境内的人造成伤害，在另一成员国对个人进行补偿后，某成员国应当对另一成员国进行补偿。

6．除了第 5 段所规定的情形，在不影响行使相对于第三人权利的前提下，若出现第 1 段规定的情形，各成员国不得就第 4 段的损害向相关成员国提出损害赔偿的要求。

7．当存在联合行动的计划，而且当监管机构拒绝遵守本条第 2 段第二句所设定的责任，其他监管机构可以根据第 55 条在其境内采取临时性措施。在这种情形中，可以推定为符合第 66（1）条的紧急情况，欧盟数据保护委员会应根据第 66（2）条而作出紧急约束性决定。

第二部分 一致性

第 63 条 一致性机制

为了帮助本条例在欧盟的一致性适用，监管机构应当相互合作，以及在相关的情形下通过本部分规定的一致性机制而和欧盟委员会进行合作。

第 64 条 欧盟数据保护委员会的意见

1．当某个有权监管机构计划采取如下任何一项措施，欧盟数据保护委员会应当发布意见。为此，有权监管机构应当将决定草案告知欧盟数据保护委员会，如果：

(a)决定草案的目标是采取一系列符合第 35（4）条所规定的数据保护影响评估要求的处理操作；

(b)决定草案涉及到第 40（7）条规定的行为准则草案，或行为准则草案的修订案或延期是否符合本条例；

(c)决定草案的目标是批准符合第 41（3）条规定的委派实体，以及符合第 43（3）条规定的认证实体的标准；

(d)决定草案的目标是确定第 46（2）条（d）点和第 28（8）条规定的标准数据保护条款；

(e)决定草案的目标是批准第 46（3）条（a）点规定的合同条款；或者

(f)决定草案的目标是批准第 47 条所指的有效性公司规则。

2．任何监管机构、欧盟数据保护委员会或欧盟委员会的主席都可以提出要求，为了给出意见——特别是当有权监管机构不遵守第 61 条规定的相互协助的责任或第 62 条规定的联合行动时——可以对任何关乎一般性使用的事项，或在不止一个成员国产生影响的事项进行核查。

3．对于第 1 段和第 2 段提到的情形，欧盟数据保护委员会如果此前没有对类似事项发表过意见，应当对提交给它的事项发布一份意见。这份意见应当在八周内根据欧盟数据保护委员会成员的简单多数来决定。考虑到主要事项的复杂性，八周的期限可以再延长六周。关于第 1 段规定的按照第 5 段而在欧盟数据保护委员会中流通的决议草案，如果某成员在欧盟数据保护委员会主席所表明的合理期限内不提出异议，就应当视为同意决议草案。

4．监管机构和欧盟数据保护委员会应当及时以电子化手段，使用标准化的格式将任何相关信息进行沟通。此类信息可以是事实的总结、决议草案、采取此类必要措施的理由，以及其他相关机构的观点。

5．欧盟数据保护委员会的主席应当及时通过电子手段：

(a)通过标准化格式将任何已经获知的相关信息告知欧盟数据保护委员会和欧盟委员会的成员。如有需要，欧盟数据保护委员会的秘书应当提供相关信息的翻译；并且

(b)将意见告知第 1 段和第 2 段规定的监管机构和欧盟委员会，并公开意见。

6．在第 3 段规定的期间内，有权监管机构不应当采用第 1 段所规定的决议草案。

7．第 1 段中所规定的监管机构应当最大限度地考虑欧盟数据保护委员会的意见，而且应在收到意见的两周内以电子方式告知欧盟数据保护委员会的主席，其是否会维持或修改其决议草案，以及修改后的决议草案——如果有的话。

8．当相关监管机构在本条第 7 段规定的期限内通知委员会主席，其并无意遵守委员会的所有意见或意见的一部分，并且提供了相关理由，此种情形下第 65（1）条应当适用。

第 65 条 欧盟数据保护委员会的纠纷解决

1．为了确保在个案中对本条例的正确与融贯适用，欧盟数据保护委员会应当在如下情形中做出有约束力的决定：

(a)在第 60（4）条规定的情形中，相关监管机构对领导性机构的草案决定提出了相关与合理的反对，或者领导性机构驳回了反对，认为其不相关或不合理。约束性决定应当涉及相关与合理反对所涉及的所有事项，特别是当其存在违反本条例的情形；

(b)对于哪个监管机构有权管辖主要营业机构存在不同意见；

(c)在第 64（1）条规定的情形中，有权监管机构并不请求获得欧盟数据保护委员会的意见，或者并不遵守欧盟数据保护委员会按照第 64 条发布的意见。在这种情形下，任何相关监管机构或欧盟数据保护委员会都可以将此事项告知欧盟数据保护委员会。

2．三分之二多数的欧盟数据保护委员会成员在将主体事项转交后，应当在 1 个月以内做出第 1 段所规定的决定。考虑到主体事项的复杂性，这个期间可以再

延长一个月。第 1 段所规定的决定应当是合理的，应当告知领导性监管机构和所有相关监管机构，并且对它们具有约束力。

3．当欧盟数据保护委员会无法在第 2 段所规定的期限内做出决定，其应当以欧盟数据保护委员会成员简单多数的方式在第 2 段所规定的第二个月的期限结束后的两星期内做出决定。如果欧盟数据保护委员会成员的投票刚好完全分裂，那么决定将根据主席的投票而做出。

4．在第 2 段和第 3 段所规定的期限内，相关监管机构不应当对根据第 1 段而提交给欧盟数据保护委员会的主体事项做出决定。

5．欧盟数据保护委员会的主席应当及时将第 1 段所规定的决定告知相关监管机构。这也就告知了欧盟委员会。在监管机构告知第 6 段规定的最终决定后，决定应当在欧盟数据保护委员会的网站上及时发表。

6．领导性监管机构或者收到申诉的监管机构应当根据本条第 1 段所规定的决定性基础及时做出最终决定，至迟应当在欧盟数据保护委员会告知其决定后的一个月以内做出。领导性的监管机构或收到申诉的监管机构应当向欧盟数据保护委员会报告其将该决定告知控制者或处理者以及数据主体的时间。相关监管机构的最终决定应当根据第 60（7）（8）（9）条的条款而做出。最终决定应当涉及本条第 1 段所规定的决定，而且应当具体说明，本条第 1 段所规定的决定将会根据本条第 5 段而在欧盟数据保护委员会的网站上发表。最终决定应当附上本条第 1 段所规定的决定。

第 66 条 紧急程序

1．在例外情形中，当相关监管机构认为有必要对保护数据主体的权利与自由采取紧急行动，其可以通过第 63、64 和 65 条规定的一致性机制或第 60 条规定

的程序来进行克减，立即采取在其境内一段时间内——不超过 3 个月——具有法律效力的临时性措施。监管机构应当及时将采取这些措施的手段与原因告知其他相关监管机构、欧盟数据保护委员会与欧盟委员会。

2．当监管机构采取符合第 1 段的措施，以及考虑亟需采用的最终措施，其可以请求欧盟数据保护委员会出具一份紧急意见或紧急约束性决定，并说明提出此请求的原因。

3．如果有必要对保护数据主体的权利与自由采取紧急行动，而有权监管机构却没有采取合适措施，任何监管机构都可以向欧盟数据保护委员会请求一份紧急意见或紧急约束性决定，说明提出此请求的原因，包括需要采取紧急行动的原因。

4．对于第 64（3）条和第 65（2）条规定的的克减，欧盟数据保护委员会成员的简单多数应当在两个星期内做出本条第 2 段和第 3 段规定的紧急意见或紧急约束性决定。

第 67 条 信息交换

对于监管机构之间、监管机构与欧盟数据保护委员会之间以电子方式进行的信息交换，特别是对于第 64 条规定的标准化格式，欧盟委员会可以进一步制定细化的实施性法案。

这些实施性法案应当根据第 93（2）条规定的验证程序制定。

第三部分 欧盟数据保护委员会

第 68 条 欧盟数据保护委员会

1．欧盟数据保护委员会特此被设立为欧盟的一个机构，而且将具有法人身份。

2．欧盟数据保护委员会的代表是其主席。

3．欧盟数据保护委员会应当包括每个成员国的每个监管机构的首长、欧盟数据保护监管者的首长，或者他们的代表。

4．当一个成员国内不止一个监管机构负责监控对本条例条款的适用，应当按照成员国的法律任命一个联合代表。

5．欧盟委员会应当有权参与欧盟数据保护委员会的活动与会议，但没有投票权。欧盟委员会应当委任一名代表。欧盟数据保护委员会的主席应当将其活动告知欧盟委员会。

6．对于第 65 条规定的情形，只有当决议涉及到适用于和本条例规定有实质性对应的欧盟机构、实体、办公室、规制机构的原则和规则时，欧盟数据保护监管者才具有投票权。

第 69 条 独立性

1．当根据第 70 条和第 71 条履行其任务或行使其权力时，欧盟数据保护委员会应当保持其独立性。

2．在不影响第 70（1）条（b）点和第 70（2）条所规定的欧盟委员会的请求的前提下，欧盟数据保护委员会在履行其任务或行使其权力时，应当避免从任何人那里获取指示。

第 70 条 欧盟数据保护委员会的任务

1．欧盟数据保护委员会应当确保对本条例的一致性适用。为了实现这一目的，在相关情形中，欧盟数据保护委员应当主动或根据欧盟委员会的请求而采取如下行动：

(a)在不影响全国性监管机构的任务的前提下，确保在第 64 条和 65 条所规定的情形中正确适用本条例；

(b)对欧盟数据保护相关的所有事项，包括对本条例的修改动议，向欧盟委员会提供建议；

(c)对为制定约束性公司规则而在控制者、处理者和监管机构之间进行的信息交换的格式与程序向欧盟委员会提供建议；

(d)从第 17（2）条规定的公众可以获取的通讯服务中擦除个人信息的链接、备份或复制品，对这种活动的程序发布指导方针、建议和最佳操作；

(e)主动或根据其成员的请求，或根据欧盟委员会的请求核查涉及本条例适用的任何问题，为了鼓励对本条例的适用，发布指导方针、建议和最佳操作；

(f)为了进一步细化第 22（2）条规定的基于用户画像的决策的标准和条件，发布符合本段（e）点的指导方针、建议和最佳操作；

(g)为了认定个人数据泄露，确定是否存在第 33（1）、（2）条所规定的无理拖延，以及控制者或处理者是否需要告知个人数据泄露，发布符合本段（e）点的指导方针、建议和最佳操作；

(h)对于个人数据违法可能会对第 34（1）条规定的自然人的权利与自由带来高风险的情形，发布符合本段（e）点的纲领、建议和最佳操作；

(i)对于符合控制者所遵守的约束性公司规则、处理者所遵守的约束性公司规则的数据转移，以及符合为了保证第 47 条规定的对数据主体的个人数据保障而采取的必要措施的个人数据转移，为了细化此类转移的标准和要求，发布符合本段（e）点的指导方针、建议和最佳操作；

(j)为了进一步细化第 49（1）条规定的个人数据转移所需要的标准和要求，发布符合本段（e）点的指导方针、建议和最佳操作；

(k)对于涉及第 58（1）、（2）、（3）条规定的适用措施和确定第 83 条规定的行政处罚，为监管机构起草指导方针；

(l)对本段（e）点和（f）点规定的指导方针、建议和最佳操作的实际运用进行审查；

(m)对自然人设报告侵犯本条例的行为，为其设立符合第 54（2）条的一般程序，，发布符合本段（e）点的指导方针、建议和最佳操作；

(n)鼓励起草行为准则，设立符合第 40 条和第 42 条的数据保护认证机制、数据保护印章和标记；

(o)对认证机构进行委任，根据第 43 条而进行阶段性审查，对符合第 43（6）条的委任机构、符合第 42（7）条而在第三国设立的被认证的控制者或处理者进行持续性的公共登记；

(p)为了委任第 42 条规定的认证机构而细化第 43（3）条规定的要求；

(q)向欧盟委员会提供关于第 43（8）条规定的验证要求的意见；

(r)向欧盟委员会提供关于第 12（7）条规定的图标的意见；

(s)评估第三国或国际组织的保护程度，包括评估第三国、某个地区、或该第三国的一个或多个特定部门，或国际组织是否仍然提供足够程度的保护。为了实现这一目的，欧盟委员会应当向欧盟数据保护委员会提供所有必要的记录，包括和该第三国政府的进行的涉及到第三国、某个地区、或该第三国的一个或多个特定部门，或国际组织的通信。

(t)发布按照第 64（1）条规定的一致性机制而做出的关于监管机构的决议草案，按第 64（2）条提交的事项，以及发布根据第 65 条，包括第 66 条规定的约束性决定。

(u)促进监管机构之间的合作，有效的双边或多边信息交换，以及最好的实践；

(v)促进共同培训项目，协助监管机构之间以及——如果适用的话——监管机构与第三国监管机构或国际组织之间的人员交换；

(w)促进与全球数据保护监管机构的知识交流、数据保护立法的记录与实践。

(x)发布关于根据第 40（9）条在欧盟层面起草的行为准则的意见；以及

(y)对于监管机构和法庭做出的决定以及根据一致性机制所处置的事项，保持一份公众可以访问的电子登记。

2．当欧盟委员会请求欧盟数据保护委员会提供意见，欧盟委员会可以在考虑事项的紧急程度后表明期限要求。

3．欧盟数据保护委员会应当将其意见、指导纲领、推荐以及最佳操作告知欧盟委员会和第 93 条规定的理事会，而且应当将它们公开。

4．如果适用的话，欧盟数据保护委员会应当咨询当事人，給与他们在一段合理期限内进行评论的机会。在不影响第 76 条的前提下，欧盟数据保护委员会应当将咨询程序的结果公之于众。

第 71 条 报告

1．对于欧盟内部、相关第三国以及国际组织中的数据处理活动，若涉及自然人的保护，欧盟数据保护委员会应当起草年度报告。报告应当公开，而且应当传输给欧洲议会、欧盟理事会和欧盟委员会。

2．年度报告应当包括第 70（1）条（l）点规定的对指导方针、建议和最佳操作的实际运用进行审查，以及第 65 条规定的约束性决议。

第 72 条 程序

1．欧盟数据保护委员会应当通过其成员的简单多数做出决定，除非本条例有相反规定。

2．欧盟数据保护委员会应当以其成员的三分之二多数制定程序规则，组建其自身的操作机制。

第 73 条 主席

1．欧盟数据保护委员会应当通过简单多数的方式从其成员中选举一位主席、两位副主席。

2．主席以及副主席职位的任期应当是 5 年，可以连任一届。

第 74 条 主席的任务

1．主席具有如下任务：

(a)召集欧盟数据保护委员会的会议，准备会议议程；

(b)将委员会根据第 65 条而做出的决定告知第 65 条规定的领导性监管机构和相关监管机构；

(c)保证欧盟数据保护委员会任务的及时履行，特别是和第 63 规定的一致性机制相关的任务。

2．欧盟数据保护委员会应当在其程序规则中对主席与副主席的任务分工进行分配。

第 75 条 秘书

1．欧盟数据保护委员会应当有一名秘书，其应当由欧盟数据保护监督者来任命。

2．秘书应当严格按照欧盟数据保护委员会主席的指示履行其职责。

3．欧盟数据保护监管者的员工，如果涉及履行到本条例赋予给欧盟数据保护委员会的任务，应当与涉及履行赋予给欧盟数据保护监管者的任务的员工遵守不同的报告程序。

4．在适用的情况下，欧盟数据保护委员会和欧盟数据保护监管者应当撰写与发布一份实施本条的谅解备忘录，确定它们之间合作的条款，在涉及履行本条例赋予给欧盟数据保护委员会的任务时，谅解备忘录适用于欧盟数据保护监管者的员工。

5．秘书应当向欧盟数据保护委员会提供分析、管理与后期支持。

6．秘书应当对如下事项负责：

(a)欧盟数据保护委员会的日常事务；

(b)欧盟数据保护委员会、欧盟数据保护委员会主席与欧盟委员会之间的交流；

(c)与其他机构及公众的交流；

(d) 内部交流与外部交流中对电子手段的使用；

(e)对相关信息的翻译；

(f)对欧盟数据保护委员会会议的准备与跟踪；

(g)准备、起草与发布欧盟数据保护委员会对监管机构之间分歧的意见与决定，以及其他文本。

第 76 条 机密性

1．欧盟数据保护委员会若认为根据程序规则的要求，有必要秘密开展某项讨论活动，那么该讨论活动就应当严格保密。

2．访问提交给欧盟数据保护委员会的成员、专家与第三方代表的文件，应当遵守欧洲议会和欧盟理事会的(EC) No 1049/2001 条例[1]。

第八章 救济、责任与惩罚

第 77 条 向监管机构提起申诉的权利

1．在不影响任何其他行政或司法救济的前提下，每个数据主体都有向监管机构进行申诉的权利，这尤其适用于以下地点的监管机构：数据主体所属的成员国或经常居住地、工作地、或数据主体认为处理其个人数据违反本条例的发生地。

2．收到申诉的监管机构应当告知申诉者申诉的进展和结果，包括符合第 78 条的司法救济的可能性。

第 78 条 针对监管机构的有效司法救济权

1．在不影响其他任何行政或司法救济的前提下，任何自然人或法人都有权对关乎他们的监管机构的有法律约束力的决定获得有效的司法救济。

2．在不影响其他任何行政或司法救济的前提下，如果根据第 55 条和第 56 条的有权监管机构不处置申诉，或者在三个月内没有向数据主体告知第 77 条规定的申诉的进展或结果，任何自然人或法人都有权获得有效的司法救济。

3．针对监管机构的法律诉讼应当在监管机构所在的成员国的法庭提起。

4．如果针对监管机构决定的法律诉讼发生在欧盟数据保护委员会根据一致性机制而做出意见或决定之前，监管机构应当将其意见或决定告知法院。

第 79 条 针对控制者或处理者的有效司法救济权

1．在不影响其他任何行政或司法救济的前提下，包括在不影响第 77 条规定的向监管机构提交申诉的前提下，任何数据主体认为，由于违反本条例而处理其个人数据，导致其被本条例所赋予的权利被侵犯，在这些情形下其都有获取司法救济的权利。

2．针对控制者或处理者的法律诉讼应当在它们拥有机构的成员国的法庭提起。在其他情形下，此类法律诉讼可以在数据主体的经常居住地的法庭提起，除非控制者或处理者是成员国行使其公共权力的公共机构。

第 80 条 对数据主体的代表

1．数据主体有权委托非盈利机构、实体或协会代表其行使第 77、78、79 条规定的权利，以及在成员国法律规定的情形下，代表其行使第 82 条规定的获得赔偿的权利。非盈利机构、实体或协会应具备如下条件：按照成员国法律设立，其章程目标是实现公共利益，在为了保护数据主体的权利与自由而代表个人提起申诉方面表现积极。

2．不论数据主体是否委托，成员国都可以规定，本条第 1 段所规定的任何机构、组织或协会如果认为本条例所规定的数据主体的权利已经因为处理而受到侵犯，都有权在成员国向第 77 条规定的有权监管机构提起申诉，行使第 78 条和第 79 条规定的权利。

第 81 条 法律诉讼的中止

1．当一个成员国的有管辖权的法院获知，另一成员国的法院准备对涉及同一个控制者或处理者处理的同一主要事项进行判决，该法院应当通知另一成员国的法院已经存在此类法律程序。

2．当另一成员国法院准备对涉及同一个控制者或处理者处理的同一主要事项进行判决，除了首先接收案件的法院，所有有权审理的法院都可以停止其法律程序。

3．在那些诉讼等待初审的情形中，如果首先接收案件的法院对涉及的活动具有管辖权而且其法律允许合并审理，所有除了首先接收案件的法院都可以基于相关一方的申请而拒绝管辖。

第 82 条 获取赔偿的权利与责任

1．任何因为违反本条例而受到物质或非物质性伤害的人都有权从控制者或数据者那里获得对损害的赔偿。

2．任何涉及到处理的控制者都应当对因为违反本条例的处理而受到的损害承担责任。对于处理者，当其没有遵守本条例明确规定的对处理者的要求，或者当其违反控制者的合法指示时，其应当对处理所造成的损失负责。

3．控制者或处理者如果证明自己对引起损失的事件没有任何责任，那么其第 2 段所规定的责任可以免除。

4．当不止一个控制者或处理者，或控制者与处理者同时涉及到同一处理，而且它们对第 2 段和第 3 段规定的处理所引起的所有损失承担责任，每个控制者或处理者都应当对损失负有连带责任，以便保证对数据主体的有效赔偿。

5．当控制者或处理者已经根据第 4 段的规定对所受损失进行全额赔偿，该控制者或处理者可以按照第 2 段所规定的条件，要求另一控制者或处理者返回其造成的那部分损失。

6．为了行使其获得赔偿的权利，根据第 79（2）条的规定，应当在成员国认可的有管辖权的法院提起诉讼请求。

第 83 条 行政罚款的一般条件

1．.每个监管机构都应当保证，其根据本条而对第 4、5、6 条所规定的违反本条例的行为进行罚款，在每个案件中都应当是有效的、成比例的和劝诫性的。

2．根据每个案件的具体情形，行政处罚应当在第 58（2）条的（a）至（h）点以及（j）点规定的措施基础上进行追加，或者应当代替这些措施。当在每个具体案件中决定是否应当进行行政处罚，以及决定行政处罚的金额，应当充分考虑如下因素：

(a)结合相关处理的性质、范围或目的，被影响的数据主体的数量以及损害程度而确定的违法的性质、严重性与持续时间；

(b)违法的性质是基于故意还是过失；

(c)控制者或处理者为了减轻数据主体损失而采取的所有行动；

(d)结合控制者或处理者采取的符合第 25 条和第 32 条的技术性与组织性措施而认定的控制者或处理者的责任程度；

(e)控制者或处理者之前的所有相关违法行为；

(f)为了纠正违法行为和减轻违法所造成的可能负面影响而和监管机构进行合作的程度；

(g)为违法行为所影响的个人数据类型；

(h)监管机构得知违法行为的方式，特别是控制者或处理者是否对违法行为进行了报告，以及在何种程度上进行了报告；

(i)如果对同一主题事项已经对控制者或处理者发布第 58（2）条规定的措施，对这些措施是否遵守；

(j)遵守符合第 40 条的已生效的行为准则或符合第 42 条的已生效的认证机制；以及

(k)对于案件情形可以适用的所有加重或减轻因素，例如因为违法而直接或间接导致的经济收益、避免的损失。

3．如果控制者或处理者故意或过失性地因为同一或相关的处理操作而违反本条例的条款，行政罚款的总额不应当超过最严重违法所确定的额度。

4．违反如下条款，应当按第 2 段的规定施加最高 10 000 000 欧元的行政罚款，如果是企业的话，最高可处相当于其上一年全球总营业额 2%的金额的罚款，两者取其高的一项进行罚款：

(a)第 8，11，25，26，27，28，29，30，31，32，33，34，35，36，37，38，39，42 和 43 条规定的控制者和处理者的责任；

(b)第 42 条和第 43 条规定的认证机构的责任；

(c)第 41（4）条规定的监管机构的责任。

5．违反如下条款，应当按第 2 段的规定施加最高 20 000 000 欧元的行政罚款，如果是企业的话，最高可处相当于其上一年全球总营业额 4%的金额的罚款，两者取其高的一项进行罚款：

(a)处理的基本原则，包括第 5、6、7 和 9 条规定的同意的条件；

(b)第 12 条至 22 条规定的数据主体的权利；

(c)第 44 条至第 49 条规定的将个人数据转移到第三国或一个国际组织的接收者；

(d)所有第九章规定的符合成员国法律的责任；

(e)违反监管机构根据第 58（2）条对处理所发布的命令、或暂时性或确定性的限制，或对数据流动的中止，或违反第 58（1）条拒绝提供访问。

6．违反第 58（2）条规定的监管机构发布的命令，应当按第 2 段的规定施加最高 20 000 000 欧元的行政罚款，如果是集团的话，可以施加最高前一年全球总营业额 4%的罚款，两者取其高的一项进行罚款。

7．在不影响符合第 58（2）条的监管机构的矫正权力的前提下，每个成员国都可以制定规则，确定在什么情况下对在其境内设立的公共机构和实体进行行政处罚。

8．监管机构行使本条所规定的权力，应当采取符合欧盟和成员国法律所规定的合适的程序性保障，包括有效的司法救济和正当程序。

9．当成员国的法律体系并不提供行政处罚，本条可以以如下方式适用：可以通过有权监管机构提出行政处罚，然后有职权的全国性法院进行适用，同时，应保证那些法律救济是有效的，而且这些法律救济与监管机构所施加的行政处罚具有同等效力。不论在何种情形中，所施加的处罚必须是有效的、成比例的和劝诫性的。那些成员国应当[在本条例生效两年内]将根据本段所制定的法律条款、所有后续的修正性法律或影响它们的法律修订及时告知欧盟委员会。

第 84 条 惩罚

1．成员国应当制定可适用于违反本条例的其他惩罚的规则，特别是对于那些不受第 83 条规定的行政处罚约束的违法行为，成员国应当制定必要措施保证这些惩罚规则得到执行。此类惩罚应当是有效的、成比例的和劝诫性的。

2．对于符合第 1 段所制定的法律，每个成员国的应当[在本条例生效的两年内]将其法律条款告知欧盟委员会，而且应当及时告知影响条款的后续修订。

第九章 和特定处理情形相关的条款

第 85 条 处理、表达自由与信息

1．成员国应当通过制定法律调和符合本条例制定的个人数据保护权与表达自由权与信息权，包括调和为了新闻目的和学术、艺术或文学表达目的而进行的处理。

2．对于出于新闻目的和学术、艺术或文学表达目的而进行的处理，如果对于调和符合本条例制定的个人数据保护权与表达自由权与信息权有必要，成员国应当对第二章（原则）、第三章（数据主体的权利）、第四章（控制者和处理者）、第五章（个人数据转移到第三国或国际组织）、第六章（独立监管机构）、第七章（合作与一致性）和第九章（特定数据处理的情形）的规定进行豁免或克减。

3．每个成员国都应当将其按照第 2 段所制定的法律条款告知欧盟委员会，而且应当将所有后续的修正性法律或影响它们的法律修订及时告知欧盟委员会。

第 86 条 处理与公众对官方文件的访问

为了调和公众对官方文件的访问与本条例规定的个人数据保护权，对于公共机构或公共实体或为了实现公共利益而履行任务的私人实体所拥有的官方文件中的个人数据，机构或实体可以根据成员国为机构或实体而制定的法律而公开。

第 87 条 对全国性身份识别号码的处理

成员国可以对处理全国性身份识别号码或其他一般性识别标识的特定情形做出规定。在这种情形下，只有对本条例规定的数据主体的权利与自由采取适当安全保障，才能使用全国性身份识别号码或其他一般性识别标识。

第 88 条 雇佣语境下的处理

1．多个成员国可以通过法律或通过协定制定特定规则，以保证在雇佣语境下处理雇员个人数据保证其权利与自由。这在如下情形中尤其适用：为了招聘、履行雇佣合同，包括法律或集体合同规定的免除合同；对工作的管理、计划与组织；工作场所的合理性与多样性；工作中的健康与安全，对员工与顾客财产的保护；为了行使和享受雇佣相关的权利与收益；以及为了终止雇佣关系。

2．此类规则应当包括为保障数据主体人身尊严、正当利益与基本权利的合适与特定的措施。这在涉及到如下事项时尤其适用：处理的透明性；在一群企业中转移个人数据；或进行联合经济活动的一群企业和工作场所的监管系统。

3．每个成员国应当[在本条例生效的两年内]将其按照第 1 段所制定的那些法律条款告知欧盟委员会，而且应当及时告知影响条款的后续修订。

第 89 条 为了实现公共利益、科学或历史研究或统计目的处理中的安全保障与克减

1．为了实现公共利益、科学或历史研究或统计目而处理，应当采取符合本条例的恰当防护措施，保障数据主体的权利与自由。这些防护措施应当确保，为了保证数据最小化原则，已经采取技术与组织性的措施。这些措施可以包括匿名化，如果匿名化也能实现上诉目的。如果在进一步处理中实现对数据主体无法识别也可以实现上诉目的，那就应当采取这种方式处理。

2．对于为了实现公共利益、科学或历史研究或统计目的处理，成员国的法律可以按照本条第 1 段所规定的情形与防护措施对第 15、16、18、21 条所规定的权利进行克减——如果此类权利可能彻底阻碍或严重阻碍实现上述目的，而此类克减对于实现上诉目的是必要的。

3．当个人数据处理是为了实现公共利益，欧盟或成员国的法律可以按照本条第 1 段所规定的情形与防护措施对第 15、16、18、19、20 和 21 条规定的权利进行克减——如果此类权利可能彻底阻碍或严重阻碍实现上述目的，而此类克减对于实现上诉目的是必要的。

4．如果第 2 段和第 3 段所规定的处理还有其他目的，克减将只适用于为了实现第 2 段和第 3 段中所规定的目的的处理。

第 90 条 保密责任

1．成员国可以制定特定的规则，对第 58（1）条（3）和（f）点所规定的、和作为主体的控制者或处理者相关的、全国性有权机构所设立的监管机构的权力进行规定，如果有必要对个人数据保护与保守秘密进行调和与比例性保护，此特定规则可以施加职业性秘密保守责任或其他同等责任。只有在那些保守秘密责任所涉及的活动中或因为此类活动而接收个人数据，此类规则才适用于控制者或处理者。

2．每个成员国的应当[在本条例生效的两年内] 将其按照第 1 段所制定的那些法律条款告知欧盟委员会，而且应当及时告知影响条款的后续修订。

第 91 条 现有的的对教会和宗教协会的数据保护规则

1．在本条例生效后，对于适用于某成员国境内教会、宗教协会或团体的保护自然人在处理相关中的综合性规则，如果它们和本条例保持一致，仍然应当适用。

2．对于那些适用符合第 1 段的综合性规则的教会和宗教协会，其应当接受一个独立监管机构的监管，如果其满足本条例第六章规定的条件，这种独立监管机构可以是特别指定的。

第十章 授权法案与实施性法案

第 92 条 对授权的行使

1．欧盟委员会享有授权法案的制定权，此权力受本条所规定的条件所约束。

2．第 12（8）条和 43（8）条所规定的授权应当[在本条例生效后]的一段不确定的时间内赋予给欧盟委员会。

3．第 12（8）条和 43（8）条所规定的授权可以随时被欧洲议会或欧盟理事会撤销。撤销决定应当终止决定所特别指明的授予性权力。撤销决定生效日是欧盟官方杂志发布后的第二天或决定所特别标明的日期。撤销决定不应影响任何已经生效的授权性法案。

4．欧盟委员会一旦制定授权性法案，其应当立刻同时告知欧洲议会和欧盟理事会。

5．根据第 12（8）条和第 43（8）条而指定的授权性法案，只有欧洲议会或欧盟理事会在其收到通知后三个月内都没有表达反对，或者在三个月内欧洲议会或欧盟理事会已经告知欧洲委员会它们不会反对，其才能生效。如果欧洲议会或欧盟理事会提出延期，这个期间可以再延长三个月。

第 93 条 委员会程序

1．欧盟委员会应当有一个小组对其进行协助。该小组应当是(EU) No 182/2011 条例所规定的小组。

2．涉及到此段时，(EU) No 182/2011 指令第 5 条应当适用。

3．涉及到此段时，与(EU) No 182/2011 指令第 5 条配合的(EU) No 182/2011 指令第 8 条应当适用。

第十一章 最后条款

第 94 条 95/46/EC 指令的废止

1．在[本条例生效后的两年]后 95/46/EC 指令将被废止。

2．当参照废止指令时，应当通过参照本条例来进行解释。对于参照工作小组在 95/46/EC 指令第 29 条所规定的处理个人数据中个人保护，这应当以参照本条例所规定的欧盟数据保护委员会来进行解释。

第 95 条 与 2002/58/EC 的关系

在欧盟的公共通讯网络中提供公众可获取的电子通讯服务的情形中，对于2002/58/EC 指令已经施加特殊责任的事项，本条例不应再对同一事项再向自然人或法人施加额外责任。

第 96 条 和之前已经达成的协议的关系

对于[在此条例生效]之前的，符合[在此条例生效]之前所制定的法律的，涉及到将个人数据传输到第三国或国际组织的成员国之间已经达成的国际性协议，在其被修改、替代或撤销之前，应当一直具有效力。

第 97 条 委员会报告

1．在[本条例生效后的四年后]，以及在这之后的每四年，欧盟委员会应当向欧洲议会和欧盟理事会提交一份对本条例的评价与审查。该报告应当公之于众。

2．在第 1 段所规定的评价与审查情形中，欧盟委员会应当尤其检查如下事项的适用与运作：

(a)第五章规定的将个人数据转移到第三国或国际组织，特别是按照本条例第 45（3）条而做出的决定，以及根据 95/46/EC 第 25（6）条而做出的决定；

(b)第七章规定的合作与一致性。

3．为了实现第 1 段的目的，欧盟委员会可以要求成员国和监管机构提供相关信息。

4．为了进行第 1 段和第 2 段规定的评价与审查，欧盟理事会应当考虑欧洲议会、欧盟理事会以及其他相关实体与生产商的立场与调查。

5．在必要的情形下，欧盟委员会应当提交修改本条例的合适动议，特别是如果考虑了信息科技的发展以及信息社会中的发展状态。

第 98 条 对欧盟其他数据保护法案的审查

如果合适的话，欧盟委员会应当提交立法性动议，以便对欧盟的其他个人数据保护法案进行保护，以便保证在处理中对自然人进行一致与一致性的保护。这尤其应当涉及到欧盟机构、实体、办公室和规制机构处理中和自然人保护相关的规则，以及此类数据的自由流动。

第 99 条 生效与适用

1．本条例的生效时间是其在欧盟官方杂志发布后的二十天后。

2．其适用时间是[本条例生效后的两年后]。

本条例的所有条款都具有约束力，而且应当直接适用于成员国。