一张表读懂《个人信息安全规范》与 GDPR 的异同

詹昊、宋迎、吴院渊、韦飞

2018 年 5 月 25 日施行的欧盟《通用数据保护条例》（以下简称 GDPR）被视为当前最为全面、严格的数据保护法案。与其同月生效的《信息安全技术 个人信息安全规范》(GB/T 35273—2017)（以下简称《个人信息安全规范》或《规范》）也是目前国内个人信息保护制度中最完善的规范性文件。

尽管《个人信息安全规范》只是一部推荐性国家标准，但是其定位是我国个人信息保护工作的基础性标准，在相应法律法规暂未明确规定的前提下，将是个人信息保护工作合规性的重要参考标准，而且也为今后相关领域的立法活动奠定一定基础。

《个人信息安全规范》与 GDPR 有很多相似的地方，往往被称为“中国版 GDPR”，但在具体规制个人信息的范围、方式和有关合规性要求上，两者还是有各自的特点。对于跨国企业尤其涉及欧盟业务的企业而言，建立适应跨境业务的数据合规体系需综合考虑各法域的监管要求，因此厘清二者的异同具有一定的实践意义。

为此，我们将二者在一些事项上有共同或相似规定的条款以表格形式列出，不涉及各自单独规范的一些情形。后续我们将持续关注《个人信息安全规范》在执法、司法实践中落地的参考适用情况，并将对企业涉及 GDPR 的合规建设提出更多建议。

项目	个人信息安全规范	GDPR
1. 个人信息的用词	personal information	personal data
2. 个人信息的定义	以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特	任何与已识别或可识别的自然人（数据主体）相关的信息；可识别的自然人是指可以被直接或间

	定自然人活动情况的各种信息。 包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。	接地予以识别的自然人，特别是通过参考具体识别信息进行识别，如姓名、身份证号码、地理信息、在线身份识别信息、或该自然人一个或多个的身体、生理、遗传、心理、经济、文化或社会身份等。
3. 特殊数据的定义（个人敏感信息）	“个人敏感信息”是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。 包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。	“特殊类型的个人数据”指： 1、披露种族或人种、政治意见、宗教或哲学信仰或贸易联盟会员的个人数据； 2、基因数据、用以识别自然人的生物特征的识别数据、涉及健康或自然人的性生活或性倾向的个人数据。
4. 适用的行为与客体	规范开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动。	全部或部分以自动化方式处理的个人数据，亦适用于其他以非自动化方式处理而构成档案系统的一部分或旨在构成档案系统的一部分的个人数据。
5. 适用的地域范围	未明确规定，但作为中国国家标准，通常不具有域外效力。	1、适用于数据控制者或处理者在欧盟境内的机构所进行的个人数据处理活动，而无论该处理是否发生在欧盟境内的； 2、设立与欧盟境外的数据控制者或处理者向欧盟境内的数据主体提供商品或服务或对数据主体在欧盟内的发生的行为进行监控。 3、设立于欧盟境外，但根据国际公法数据控制者进行的数据

		处理活动适用欧盟成员国法律。
6. 控制者	**“个人信息控制者”**：有权决定个人信息处理目的、方式等的组织或个人。	**“数据控制者”**：单独或与他人共同决定个人数据处理目的与方法的自然人或法人、公共机关、部门或其他机构。该数据处理目的与方法依据欧盟法或成员国法决定。数据控制者认定的具体标准可由欧盟法或成员国法规定。
7. 共同控制者	**“共同个人信息控制者”**：当个人信息控制者与第三方为共同个人信息控制者时（例如服务平台与平台上的签约商家），个人信息控制者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知。 个人信息控制者在提供产品或服务的过程中部署了收集个人信息的第三方插件（例如网站经营者与在其网页或应用程序中部署统计分析工具、软件开发工具包 SDK、调用地图 API 接口），且该第三方并未单独向个人信息主体征得收集、使用个人信息的授权同意，则个人信息控制者与该第三方为共同个人信息控制者。	**“共同数据控制者”（Joint controllers）**：两个或两个以上数据控制者共同决定处理目的及方式时，其应为共同数据控制者。共同数据控制者应以透明的方式，彼此间安排，确定其履行本条例规定的义务与责任，尤其是涉及数据主体权利的行使及数据控制者收集数据时向数据主体提供 GDPR 第 13、14 条规定的信息。但欧盟法或成员国法就数据控制者各自责任已有明文者不在此限。 上述**“安排”**（arrangement）需指定数据主体的联络点，并应适当反映共同数据控制者对于数据主体各自的角色及关系。 无论“安排”的条款如何，数据主体得依据本条例对任一数据控制者主张其权利。
8. 用户画像	通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如其职业、经济、健康、教育、个人喜好、信用、行为等方面做出分析或预测，形成其个人	以任何形式对个人数据进行的自动化处理，包括使用个人数据对自然人有关个人特征予以评估，特别是用来分析或预测有关自然人的工作表现、经济状况、健康、个人偏好、兴趣、可信度、行为、

	特征模型的过程。 进一步区分直接用户画像与间接用户画像： 1、直接用户画像：直接使用特定自然人的个人信息，形成该自然人的特征模型； 2、间接用户画像：使用来源于特定自然人以外的个人信息，如其所在群体的数据，形成该自然人的特征模型。	地点或动向等特征。
9. 收集个人信息的合法性要求	1、 不得欺诈、诱骗、强迫个人信息主体提供其个人信息； 2、 不得隐瞒产品或服务所具有的收集个人信息的功能； 3、 不得从非法渠道获取个人信息； 4、 不得收集法律法规明令禁止收集的个人信息。	合法处理个人数据须符合下列情形： 1、 数据主体同意； 2、 处理为履行合同所必须，而数据主体为该合同的一方；或在缔约前，满足数据主体要求； 3、 处理是数据控制者为遵守法定义务所必须的； 4、 处理是为保护数据主体或他人重大利益所必须的； 5、 处理是为完成涉及公共利益的任务或官方授权； 6、 处理是数据控制者或第三方为追求正当利益所必须的，但数据主体的基本权利和自由要求对该个人数据予以保护的利益超过前述正当利益除外，尤其是当该数据主体为儿童时，前述规则不予适用；本条也不适用于公共机关执行其任务时所进行的处理。
10. 同意	**“明示同意”**：个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。 肯定性动作包括个人信息主体	**“同意”**：数据主体基于其意思，通过声明或明确肯定的行动，所表示的自主、具体、知情及明确的处理与其个人数据有关的同意。 1、当处理是基于同意时，数据控

	主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”等。 需要明示同意的情形如下： 1、收集个人敏感信息； 2、超出授权范围使用个人信息的，应再次征得个人信息主体明示同意； 3、共享、转让个人敏感信息； 4、变更个人信息使用目的时，应重新取得个人信息主体的明示同意； 5、经法律授权或具备合理事由确需公开披露个人信息时。	制者应证明数据主体已同意对其个人数据的处理； 2、如数据主体作出的书面同意声明涉及其他事项，同意请求应以与其他事项清楚区分的方式呈现，并采取易懂且方便取得的形式，采用清楚简易的语言。任何违反 GDPR 的声明条款都不具约束力； 3、在评估同意的作出是否具自主性时，应特别考虑，合同的履行是否将同意不作为履行合同必需的条件。
11. 收集未成年人信息	收集年满14的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意。	如儿童未满 16 岁，需要其法定代理人授权或同意范围内合法。 在儿童法定代理人进行授权或作出同意的情况下，数据控制者应作出合理努力，运用现有技术，核实该法定代理人的同意或授权。 欧盟成员国可以法律规定低于上述规定的年龄，但不得低于 13 岁。
12. 同意的撤回	向个人信息主体提供方法撤回收集、使用其个人信息的同意授权。撤回同意后，个人信息控制者后续不得再处理相应的个人信息。撤回同意不影响撤回前基于同意的个人信息处理 对外共享、转让、公开披露个人信息，应向个人信息主体提供撤回同意的方法。	数据主体有权随时撤回其同意。撤回不影响撤回前基于该同意所进行的处理的合法性。在作出同意之前，数据主体应被告知其得随时撤回其同意。同意的撤回应与同意的作出一样容易；

13. 直接从个人信息主体收集个人信息时向信息主体履行告知义务	1、收集个人信息前，应向个人信息主体明确告知所提供产品或服务的不同业务功能分别收集的个人信息类型，以及收集、使用个人信息的规则（例如收集和使用个人信息的目的、收集方式和频率、存放地域、存储期限、自身的数据安全能力、对外共享、转让、公开披露的有关情况等）。 2、主动提供或自动采集方式收集个人敏感信息，向个人信息主体告知所提供产品或服务的核心业务功能及所必需收集的个人敏感信息，并明确告知拒绝提供或拒绝同意将带来的影响；其他附加功能，需要收集个人敏感信息时，收集前应向个人信息主体逐一说明个人敏感信息为完成何种附加功能所必需，并允许个人信息主体逐项选择是否提供或同意自动采集个人敏感信息。当个人信息主体拒绝时，可不提供相应的附加功能，但不应以此为理由停止提供核心业务功能，并应保障相应的服务质量。	数据控制者应在取得个人数据时，向数据主体下列所有信息： 1、数据控制者及其代表（如适用）的身份及联系方式； 2、数据保护官（如适用）的联系方式； 3、个人数据的处理目的及该处理的法律依据； 4、处理基于该数据控制者或第三人所追求的正当利益； 5、个人数据的接收者或接收者类型（如有）； 6、数据控制者拟将个人数据转让至第三国或国际组织的事实，以及欧委会就此是否做出充分决议，涉及转让的，告知合适或适当的保护措施及取得该副本的方式或该副本的保存地点； 7、个人数据的储存期间，或当无法告知该期间时，确定该期间所采用的标准； 8、向数据控制者请求获取、更正、删除个人数据或限制处理与数据主体相关个人数据或就处理提出异议的权利，以及数据移动的权利； 9、向监管机关提起申诉的权利； 10、提供个人数据是否为法定或合同要求，或为订立合同的必要要件，以及数据主体是否有义务提供个人数据以及未提供该数据可能产生的后果； 11、在第 22 条第 1 款及第 4 款规定的自动决策（包括画像）的情形，提供至少包括数据主体的信息处理所涉及逻辑的有意义信息，以及重要性与预设结果； 12、如数据控制者所拟进一步处理个人数据的目的与收集该个人数据的目的不同，数据控

		制者在进一步处理前，应向数据主体提供任何关于该目的及第 2 款规定的相关信息。
14. 间接获取个人信息行知义务	间接获取个人信息时： 1、应要求个人信息提供方说明个人信息来源，并对其个人信息来源的合法性进行确认； 2、应了解个人信息提供方已获得的个人信息处理的授权同意范围，包括使用目的，个人信息主体是否授权同意转让、共享、公开披露等。如本组织开展业务需进行的个人信息处理活动超出该授权同意范围，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意。	数据控制者不是自数据主体取得个人数据时应向数据主体提供如下信息： 1、数据控制者及其代表（如适用）的身份及联系方式； 2、数据保护官（如适用）的联系方式； 3、个人数据的处理目的及该处理的法律依据； 4、个人数据类型； 5、个人数据的接收者或接收者类型； 6、数据控制者拟将个人数据转让至第三国或国际组织的事实，及欧委会是否就此做出充分决议，涉及转让的，告知合适或适当的保护措施及取得该副本的方式或该副本的保存地点； 7、个人数据将被储存的期间，或在无法告知该期间时，确定该期间的标准； 8、处理是数据控制者或第三人所追求的正当利益所必须的； 9、向数据控制者请求获取、更正、删除或限制处理与数据主体相关的个人数据或就处理提出异议的权利，以及数据移动的权利； 10、向监管机关提起申诉的权利； 11、个人数据来源，及其是否可由公开途径获取； 12、在第 22 条第 1 款及第 4 款规定的自动决策（包括画像）的情形，提供至少包括数据主体的信息处理所涉及逻辑的

		有意义信息，以及重要性与预设结果。
15. 知情权	个人信息控制者应向个人信息主体提供访问下列信息的方法： 1、其所持有的关于该主体的个人信息或类型； 2、上述个人信息的来源、所用于的目的； 3、已经获得上述个人信息的第三方身份或类型。 此外，《规范》还明确规定了“隐私政策的内容和发布”，内容应包括但不限于： 1、个人信息控制者的基本情况，包括注册名称、注册地址、常用办公地点和相关负责人的联系方式等； 2、收集、使用个人信息的目的，以及目的所涵盖的各个业务功能，例如将个人信息用于推送商业广告，将个人信息用于形成直接用户画像及其用途等； 3、各业务功能分别收集的个人信息，以及收集方式和频率、存放地域、存储期限等个人信息处理规则和实际收集的个人信息范围； 4、对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及所承担的相应法律责任； 5、遵循的个人信息安全基本原则，具备的数据安全能力，以及采取的个人信息安全保护措施。 6、个人信息主体的权利和实现机制，如访问方法、更正	数据主体有权向数据控制者确认与其有关的个人数据是否正被处理，在这种情况下者，数据主体应有权获取其个人数据及下列信息： 1、处理目的； 2、个人数据类型； 3、已向或将向其批露的个人数据接收者或接收者类型，尤其是在第三国境内或国际组织的接收者； 4、如可能，个人数据的储存期间，或于无法告知该期间时，确定该期间所采用的标准； 5、向数据控制者请求更正、删除或限制处理与其相关个人数据或就处理提出异议的权利； 6、向监管机关提起申诉的权利； 7、如个人数据非从数据主体处收集所得的，关于该来源的任何充分信息； 8、自动决策（包括画像）的信息； 9、如将个人数据转让至第三国或至国际组织，告知该转让所应当采取的适当保护措施。

	方法、删除方法、注销账户的方法、撤回同意的方法、获取个人信息副本的方法、约束信息系统自动决策的方法等； 7、提供个人信息后可能存在的安全风险，及不提供个人信息可能产生的影响； 8、处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式。	
16. 收集后的保存和处理要求	1、保存时间最小化。 个人信息保存期限应为实现目的所必需的最短时间；超出上述个人信息保存期限后，应对个人信息进行删除或匿名化处理。 2、去标识化处理。 收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信息处理中不重新识别个人。	“pseudonymisation”（**化名化**）：通过对个人数据的处理，使其在不适用额外信息时，不再能够识别出特定的数据主体，但前提是该额外数据已被分开存储，并采取技术及组织措施确保该个人数据无法或不可识别出自然人。
17. 对个人信息使用的限制（包括对自动决策的约束）	1、除目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像； 2、对所收集的个人信息进行加工处理而产生的信息，能够单独或与其他信息结合识别自然人个人身份，或者反映自然人个人活动情况的，应将其认定为个人信息。对其处理应遵循收集个人信息时获得的授权同意范围；	1、数据主体有权随时拒绝对个人数据的处理，包括对其个人数据的画像。除非数据控制者证明其处理有优先于数据主体权利及自由的法律依据，或为确立、行使或保护法律上诉求。 2、以直接营销为目的处理个人数据时，数据主体有权随时就该营销涉及的画像提出异议。 3、数据主体有权不受仅基于自动化决策（包括画像）所做的对其产生法律效果或重大影响的约束，例外是： 1）为缔结或履行数据主体与数据控制者之间合同所必须； 2）欧盟法律或成员国法律明

	3、使用个人信息时，不得超出与收集个人信息时所声称的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得个人信息主体明示同意。 4、当仅依据信息系统的自动决策而做出显著影响个人信息主体权益的决定时（例如基于用户画像决定个人信用及贷款额度，或将用户画像用于面试筛选），个人信息控制者应向个人信息主体提供申诉方法。	确授权，且该法律有适当的保护措施以保护数据主体的权利、自由及正当利益； 3）数据主体明确同意。
18. 更正权	个人信息主体发现个人信息控制者所持有的该主体的个人信息有错误或不完整的，个人信息控制者应为其提供请求更正或补充信息的方法。	数据主体应有权应当有权要求数据控制者无不当迟延地更正与该数据主体相关的不准确个人数据。考虑到处理的目的，数据主体应有权完善其尚不完整的个人数据，包括以提供补充说明的方式。
19. 删除权	1、符合以下情形的，个人信息主体要求删除的，应及时删除个人信息： 1）个人信息控制者违反法律法规规定，收集、使用个人信息的； 2）个人信息控制者违反了与个人信息主体的约定，收集、使用个人信息的。 2、个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除； 3、个人信息控制者违反法律法规规定或与个人信息主	1、数据主体有权基于以下原因之一，要求数据控制者删除其个人数据，不得无故拖延，且数据控制者应有义务删除该个人数据，不得无故拖延： 1）个人数据对于收集或处理目的不再需要； 2）主体撤回其同意，且该处理已无其他法律依据的情形； 3）数据主体提出异议，且该处理无其他优先适用的法律依据； 4）该个人数据遭违法处理； 5）数据控制者为遵守欧盟法或成员国法律有义务删除个人数据； 6）个人数据是基于第 8 条第 1 款规定为提供信息社会服务所收集。

	体的约定，公开披露个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。	2、如数据控制者已将该个人数据公开，该数据控制者应在考虑现有科技及执行成本后，采取包括科技措施在内的合理步骤，就数据主体已提出删除其个人数据的链接、副本或复印件的请求通知正在处理该个人数据的数据控制者。
20. 个人信息主体获取副本的权利（可携带权）	根据个人信息主体的请求，个人信息控制者应为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将以下个人信息的副本传输给第三方： 1、 个人基本资料、个人身份信息； 2、 个人健康生理信息、个人教育工作信息。	1、 数据控制者应提供一份正在处理的个人数据副本。若数据主体要求更多副本，数据控制者得收取行政成本的合理费用。如数据主体以电子方式提出请求，除数据主体有不同要求外，应以电子方式提供该信息。 2、 在下列情形中，数据主体有权以结构化的、符合通常使用的、机器可读的形式，接收其提供予数据控制者的数据，并有权将其传输给其他数据控制者，而不受其提供个人数据的数据控制者的妨碍： 1）基于数据主体的同意； 2）处理以自动化方式进行 3、 在技术允许的情况下，数据主体应有权使该个人数据由一数据控制者直接传输予其他数据控制者。
21. 及时响应个人信息主体的要求	1、 在验证个人信息主体身份后，应及时响应个人信息主体提出的访问、更正、删除、撤回同意、注销账户、获取副本等请求，应在三十天内或法律法规规定的期限内做出答复及合理解释，并告知个人信息主体向外部提出纠纷解决的途径； 2、 对合理的请求原则上不收取费用，但对一定时期内多次重复的请求，可视情取一定成本费用；	1、 为促进本条例下数据主体权利的行使，应当规定一定的制度，包括行使请求权，以及（如适用）免费查阅、修正、删除个人数据，和对异议权的行使。数据控制者还应当允许数据主体以电子方式提出请求，特别是当个人数据是以电子方式处理时。数据控制者应当有义务及时（最迟在一个月内）就数据主体的请求做出答复，并在无法满足该等请求时给出理

	3、 如直接实现个人信息主体的请求需要付出高额的成本或存在其他显著的困难，个人信息控制者应向个人信息主体提供其他替代性方法，以保护个人信息主体合法权益。	由。 2、 若数据主体要求更多副本，数据控制者得收取行政成本的合理费用。
22. 对敏感信息的额外要求	涉及个人敏感信息的： 1、收集前应取得个人信息主体明示同意； 2、传输和存储时，应采用加密等安全措施；存储个人生物识别信息时，应采用技术措施处理后再进行存储； 3、对个人敏感信息的访问、修改等行为，宜在对角色的权限控制的基础上，根据业务流程的需求触发操作授权； 4、共享、转让个人敏感信息前，需向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型、涉及的个人敏感信息的类型、数据接收方的身份和数据安全能力，并事先征得个人信息主体的明示同意； 5、公开披露个人敏感信息前，向个人信息主体告知公开披露个人信息的目的、类型、涉及的个人敏感信息的内容，并事先征得个人信息主体明示同意。	禁止披露种族或人种、政治意见、宗教或哲学信仰或贸易联盟会员的个人数据、以及基因数据、用以识别自然人的生物特征的识别数据、涉及健康或与自然人的性生活或性倾向的个人数据。例外情形如下： 1、数据主体已明确同意为一个或多个特定目的处理其个人数据； 2、数据处理为数据控制者履行义务、行使特定权利所必需，或由欧盟法、成员国法或依据成员国法律所签署的集体协议为数据主体基本权利及利益提供适当保障所必须； 3、数据主体因身体或法律限制无法作出同意，而数据处理为保护数据主体或他人的重大利益所必须； 4、非营利组织，基于政治、哲学、宗教或工会的目的，数据处理仅涉及该组织的现有成员或过去成员，或与该组织目的有关而定期接触该组织的人员，且该等个人数据未经数据主体的同意不会对外披露； 5、对数据主体明显已自行公开的个人数据的处理； 6、数据处理为建构、行使或防御法律诉求或法院行使司法权所必须； 7、数据处理为维护重大公共利益所必须；

		8、数据处理为预防或职业医学的目的、为员工工作能力评估、医疗诊断、健康、社会保障或治疗提供、或为健康及社会保障系统及服务的管理所必须； 9、数据处理为公共卫生领域的公共利益所必须。 10、符合公告利益的存档、科学或历史研究或统计目的所必须。
23. 委托处理	1、个人信息控制者作出委托行为，不得超出已征得个人信息主体授权同意的范围； 2、个人信息控制者应对委托行为进行个人信息安全影响评估，确保受委托者具备足够的数据安全能力，提供了足够的安全保护水平； 3、受委托者应： 1）严格按照个人信息控制者的要求处理个人信息。如受委托者因特殊原因未按照个人信息控制者的要求处理个人信息，应及时向个人信息控制者反馈； 2）如受委托者确需再次委托时，应事先征得个人信息控制者的授权； 3）协助个人信息控制者响应个人信息主体基于本标准7.4至7.10提出的请求； 4）如受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件，应及时向个人信息控制者反馈； 5）在委托关系解除时不再保存个人信息. 4、个人信息控制者应对受委托者进行监督，方式包括	1、若处理由数据控制者的代表进行，数据控制者应仅任用充份保证会采取适当的技术和组织措施、使处理符合本条例要求、并确保数据主体权利保障的处理者。 2、未经数据控制者事先特殊或一般书面授权，处理者不得聘用其它处理者。如经一般书面授权，处理者应通知数据控制者任何关于增加或替换其他处理者的预期变化，从而使得数据控制者有机会对该等变化提出异议。 3、处理者的处理活动应遵守合同、欧盟法或成员国法的其他法律，该等法律对于处理者及数据控制者具有约束力，并规定处理标的及处理期间、处理本质与目的、个人数据的类型及数据主体的类别以及数据控制者的义务及权利。该合同或其他立法尤其应规定处理者。 4、当处理者代表数据控制者与他处理者联合进行特定处理活动时，应通

	但不限于； 1）通过合同等方式规定受委托者的责任和义务； 2）对受委托者进行审计 5、 个人信息控制者应准确记录和保存委托处理个人信息的情况。	过合同、欧盟法或成员国立法，使其他处理者同样遵守第 3 款规定的数据控制者与处理者之间的合同或其他立法规定的相同数据保护义务，尤其是提供充分保证其将采取适当技术及组织措施，使其处理符合本条例的要求。如其他处理者未能履行其数据保护义务，则原处理者应就其他处理者的义务对数据控制者承担完全责任。 5、 处理者遵守第 40 条规定的经核准的行为守则或第 42 条规定的经核准的认证机制的，得作为本条第 1 款及第 4 款规定的充分保证的证明。 6、 在不影响数据控制者与处理者合同的情况下，本条第 3 款及第 4 款规定的合同或其他立法得全部或部分基于第 7 款及第 8 款规定的标准合同条款。 7、 欧委会得就本条第 3 款及第 4 款规定的事项拟定标准合同条款，并遵守第 93 条第 2 款规定的检验程序。 8、 监管机关得就本条第 3 款及第 4 款规定的事项制定标准合同条款，并遵守第 63 条规定的一致性机制。 9、 第 3 款及第 4 款规定的合同或其他立法应采用包括电子形式在内的书面形式。

		10、在不影响第 82 条、第 83 条及第 84 条规定的情况下，如处理者决定处理的目的与方式违反本条例，该处理者应被视为该处理的数据控制者。
24. 控制者必须记录的内容	《规范》未集中规定记录的要求，在各条款中分别规定如下情形需要记录： 1、 授权特定人员超权限处理个人信息； 2、 个人信息控制者应准确记录和保存委托处理个人信息的情况； 3、 记录和保存个人信息的共享、转让的情况，包括共享、转让的日期、规模、目的，以及数据接收方基本情况等； 4、 记录和保存个人信息的公开披露的情况，包括公开披露的日期、规模、目的、公开范围等； 5、 个人信息安全事件，包括但不限于：发现事件的人员、时间、地点，涉及的个人信息及人数，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门； 6、 安全审计的相关	数据控制者及其代表应记录以下信息： 1、 数据控制者以及共同数据控制者（如适用）、数据控制者代表及数据保护官的名称及联系方式； 2、 处理目的； 3、 对数据主体类型及个人数据类别的描述； 4、 已经或即将获得个人数据披露的接收者类型，包括第三国或国际组织的接收者； 5、 将个人数据转让至第三国或国际组织（如适用），包括该第三国或国际组织的身份，且若为第 49 条第 1 款第 2 项规定的转让的，应包含适当保护措施的书面文件； 6、 删除不同类别的个人数据的预设时间上限（如可能）； 7、 第 32 条第 1

	记录。	款规定的技术及组织的安全措施概述（如可能）。 数据记录的要求不适用于员工人数低于 250 人以下的企业或组织，除非其所作出的处理会威胁数据主体权利及自由、处理，且该处理并非为是偶然的、或其处理包括第 9 条第 1 款规定的特殊类型的个人数据、或包括第 10 条规定涉及刑事定罪和违法犯罪的个人数据。
25. 发生个人信息安全事件时监管机构报告的机制	按《国家网络安全事件应急预案》的有关规定及时上报，报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式。	1、 当个人数据侵害发生时，数据控制者即应依第 55 条向监管机关通报，不得无故迟延，且如可能，应于发现后 72 小时内通报，但个人数据侵害未造成对自然人权利及自由的风险时，不在此限。未于 72 小时内向监管机关通报的，通报应附迟延理由。 2、 发现个人数据侵害后，处理者应通报数据控制者，不得无故迟延。
26. 发生个人信息安全事件时受影响个人知的通	应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。告知内容应包括但不限于： 1、 安全事件的内容和影响； 2、 已采取或将要采取的处置措施； 3、 个人信息主体自主防范和降低风险的建议；	1、 若个人数据侵害可能导致对自然人权利及自由的高风险，数据控制者应就个人数据侵害与数据主体进行沟通，不得无故迟延。 2、 与数据主体的沟通，应以清楚简易的语言描述个人数据侵害，并至少包括第 33 条第 3 款第 b、c、d 项的信息及措施。

	4、 针对个人信息主体提供的补救措施； 5、 个人信息保护负责人和个人信息保护工作机构的联系方式。	
27. 个人信息安全评估措施	1、 要建立个人信息安全影响评估制度，定期（至少每年一次）开展个人信息安全影响评估。 2、 此外对于需要进行评估的情形特别规定如下： 1) 委托处理。个人信息控制者应对委托行为进行个人信息安全影响评估，确保受委托者具备足够的数据安全能力，提供了足够的安全保护水平； 2) 共享、转让。共享、转让个人信息，非因收购、兼并、重组原因的，应事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施； 3) 公开披露。公开披露个人信息前应事先开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施； 4) 跨境传输。应当按照国家网信部门会同国务院有关部门制定的办法和相关标准进行安全评估。	当一种数据处理方式，尤其是采用新技术的，数据控制者应于处理前针对该处理对个人数据保护的影响进行评估。单一评估也可针对一系列呈现相似高风险操作。 实施数据保护影响评估时，应寻求数据保护官意见。 特别适用情形如下： 1、自然人系统性的及深入的个人特质评估，而该评估是基于自动处理（包括画像），且该评估的决定将对该自然人产生法律影响或其他类似重大影响； 2、大规模处理特殊类型的个人数据或刑事定罪和违法犯罪的个人数据； 3、对公众可访问区域的大规模系统性监控。
28. 责任部门与人	1、 应明确其法定	数据控制者及处理者应于下列任

员（数据保护官）	代表人或主要负责人对个人信息安全负全面领导责任； 2、应任命个人信息保护负责人和个人信息保护工作机构； 3、以下情形应设立专职的个人信息保护负责人和个人信息保护工作机构： 1）主要业务涉及个人信息处理，且从业人员规模大于200人； 2）处理超过50万人的个人信息，或在12个月内预计处理超过50万人的个人信息。	一情形中指定数据保护官： 1、除法院行使其司法权外，该处理由公共机关或机构执行； 2、数据控制者或处理者的核心活动，包括依其本质、范围及/或其目的，需要定期且系统性地大规模监控数据主体；或 3、数据控制者或处理者的核心活动包括大规模处理第9条规定的特殊类型的数据及第10条规定的刑事定罪和违法犯罪相关的个人数据。 数据控制者或处理者应公布数据保护官的联系方式，并告知监管机关。