Avature 伴您实现《个人信息保护法》(PIPL)合规之旅

关于中国《个人信息保护法》(PIPL) 您需要了解什么?

《个人信息保护法》(PIPL) 是中国迄今为止在个人信息保护领域最全面的法律。《个人信息保护法》根据《中华人民共和国宪法》制定,旨在 "保护个人信息权益","规范个人信息处理活动",以及 "促进个人信息合理使用"。

与欧盟的《通用数据保护条例》(GDPR) 相呼应,《个人信息保护法》适用于在中国境内处理自然人个人信息;或在中国境外处理中国境内自然人个人信息,以向境内个人提供产品或服务,或分析、评估境内个人行为。《个人信息保护法》从国家安全和数字主权的角度建立了个人信息处理的法律框架,这与中国目前的政策重点相一致,此外,其强调保护个人权利不被滥用也使中国与国际社会对个人隐私的保护达成更进一步的共识。

《个人信息保护法》的特点在于:强大的个人信息主体权利,对数据共享和数据传输的严格要求(包括数据本地化条款),以及对违法组织或个人的严厉处罚措施,包括责令整改,给予警告,没收非法所得,责令暂停或终止提供服务,以及罚款 (最高可达五千万元或者上一年度营业额百分之五)。《个人信息保护法》于2021年11月1日起正式生效。

若要确保合规,Avature的客户需要:

- 熟悉《个人信息保护法》的指导原则和具体要求。
- 建立旨在支持这些原则和要求的业务流程。
- 以合法合规的方式处理候选人和员工的个人信息,并确保为数据处理活动提供了充足的技术保障。

主体关系

一般来说,《个人信息保护法》主要影响两个主体:对个人信息拥有权利的主体,或者对个人信息处理负有义务的主体。当您使用Avature的服务时,这些主体具体是指:

- 个人 (即候选人/员工)
- 个人信息处理者 (即客户) 和受托人 (即Avature)

根据《个人信息保护法》,您的候选人和员工是《个人信息保护法》下的权利主体。当候选人被保留在公司的人才池中,或作为员工被管理时,他们的个人信息便需要被处理。贵公司将作为个人信息处理者,自主决定个人信息的处理目的和方法、处理的信息类型和信息保存期限。

贵公司也有责任对委托给Avature进行的第三方个人信息处理活动进行监督。

《个人信息保护法》第二十一条规定了个人信息处理者委托第三方处理个人信息的要求。请注意，个人信息是以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息（例如，姓名、地址、手机号码等）。此外，《个人信息保护法》第五十九条规定了受托人在代表个人信息处理者处理个人信息时需要履行的义务，包括(i)采取必要措施保障所处理的个人信息的安全，以及(ii)协助个人信息处理者履行法律规定的义务。

指导原则

《个人信息保护法》规定了处理个人信息的七项原则，各组织在处理个人信息时必须遵守。

合法性：处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

目的明确： 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

最小必要： 收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

公开透明：处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

准确性： 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

权责一致：个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

存储限制： 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

个人信息跨境提供

一般来说，《个人信息保护法》要求个人信息应在中国境内处理。如果有必要确需向境外提供个人信息的，则要求个人信息处理者必须：

- 向个人告知关于个人信息跨境提供的具体信息，并取得个人的单独同意（第三十九条）。

- 满足《个人信息保护法》中规定的必要条件之一 (安全评估、专业机构认证、标准合同、法律或行政法规或国家网信部门 (CAC) 规定的其他条件)。在任何情况下,个人信息处理者都必须确保境外接收方能够提供与《个人信息保护法》所要求的同等水平的保护 (第三十八条)。
- 事前进行个人信息保护影响评估 (第五十五条)。

如果处理实体是关键信息基础设施 (CII) 运营商或处理大量个人信息的实体,一般要求个人信息存储在境内。如果有必要将这些个人信息转移到境外的,须通过国家网信部门 (CAC) 的安全评估 (第四十条)。请注意,《个人信息保护法》要求个人信息保护影响评估报告和处理情况记录应当至少保存三年 (第五十六条)。

个人信息处理者的义务

根据《个人信息保护法》,对个人信息的 "处理",是指收集、存储、使用、加工、传输、提供、公开和删除个人信息 (包括通过电子或其他方式记录并自动处理的信息)。《个人信息保护法》为个人信息处理者规定了以下主要义务,以确保个人信息处理活动符合法律规定:

(i) 向个人提供信息处理的必要通知或披露;

(ii) 获得信息处理的有效法律依据,包括个人的同意;

(iii) 采取必要的安全措施,保护个人信息免遭任何未经授权的访问、泄漏、篡改或丢失;

(iv) 如适用,需遵守中国的个人信息跨境提供的规则;

(v) 如适用,任命个人信息保护负责人;

(vi) 定期进行内部合规审查;

(vii) 如适用,开展个人信息保护影响评估报告。

个人信息处理者可以将个人信息的处理委托给第三方 (即受托人)。第二十一条和第五十九条规定了各方的权利和责任。

个人信息处理者应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务。

受托人应按照约定的处理范围 (即处理目的和处理方式) 处理个人信息。如果委托合同无效或终止,受托人必须将个人信息返还给个人信息处理者或删除。受托人还应为处理活动采取必要的安全措施,并协助个人信息处理者履行《个人信息保护法》规定的义务。

人力资源的挑战和机遇

招聘和人才管理计划需收集和使用个人信息，因此在遵守《个人信息保护法》方面面临着巨大挑战。《个人信息保护法》要求在雇用最佳候选人和保护个人信息之间取得平衡。在中国境外运营但收集中国居民个人信息的Avature客户应知悉流程的复杂性将会增加，并有可能因违规而被处以极高的罚款。

然而，严格遵守《个人信息保护法》也能为您提供重要的竞争优势，因为候选人将更愿意与您分享个人信息。有了Avature作为您可信赖的数据处理者（受托人），您将可以：

- 唤醒您现有招聘系统里的沉睡简历，识别其中强有力的候选人，减少获取新人才的需要
- 更新候选人信息
- 在数据库中重新发掘人才
- 定期与人才池中的候选人联络，加强互动

Avature作为受托人能提供哪些服务

从GDPR到《加州消费者隐私法案》，多年来，Avature一直在配合客户实现类似隐私法的合规。

我们的客户包括了大小型企业、全球所有主要的咨询公司、众多在中国开展业务的美国大型银行和制造商。我们为他们成功制定并实施了高效的招聘项目，既能在全球成功招聘到心仪人才，又能保证遵守各地的数据规定。

具体到《个人信息保护法》，我们也有在中国处理数据的专业知识和丰富经验。Avature在中国提供数据本地化服务，我们采取合理的预防措施，保护数据中心的个人信息不丢失、不滥用或受到未经授权的访问、披露、更改及破坏。此外，在相关合规要求下，Avature预计在国家网信部门的跨境信息传输标准合同出台后签订该合同。

我们在系统配置能力加大了投入，开发和完善专为支持隐私法律而设计的技术功能。我们的系统具有高度适应性，因此您可以决定如何以符合法律要求的方式处理信息。 当合规要求发生变化时，我们的技术具有随机应变的能力。

我们也曾协助客户应对政府关于公民隐私投诉的问询，并成功帮助客户解决投诉问题。我们的法律团队熟知如何起草、审查和执行对现有数据保护协议的修订。

功能

我们的解决方案针对《个人信息保护法》提供了各种不同的功能，以帮助您实现合规。

征求个人同意表格： 可以管理并跟踪（通过时间戳）获取个人同意的进度。

自定义工作流： 选择加入/退出或双重选择，这能够使征求个人同意的流程自动化并定期重新评估候选人的意愿。

自动清除或删除信息： 根据您自定义的时间间隔驱动。

加密数据： 只允许有知情必要的人员访问和编辑保密数据。

可配置的安全设置： 让您的用户能够根据您的安全需求进行相应的设置。

完整的审计日志： 追踪与候选人之间的互动，包括获取同意、信息更新和信息变更的记录。

退订链接： 通过Avature发送的电子邮件中设置退订链接，以便候选人可以随时选择退订。

数据导出： 为候选人提供其信息副本。

支持与安全措施

作为《个人信息保护法》的受托人，我们的主要责任是采取必要的措施来确保个人信息的安全，并协助个人信息处理者履行其义务。为了做到这一点，我们实施了一系列技术和组织架构方面的安全措施，例如：

- 防火墙、加密措施和其他信息保护技术
- 根据不同的客户和客户的不同目的分开处理数据
- 实行角色限制，只有需要访问敏感数据的Avature员工才有权限查看相应数据

Avature的运营、政策和管理定期接受审计，以确保我们的解决方案符合并超越对世界级技术服务提供商的所有预期。

[1] 虽然Avature提供支持合规流程的功能，但我们并非律师事务所，亦不提供专业的法律意见。但是，我们一直与企业的法律部门以及招聘与人才管理团队通力合作，严谨细致地设计招聘项目的各个环节，以确保实施合规的人才项目。此外，Avature的顾问已为众多在中国运营业务的客户的招聘项目实施提供了支持，并根据客户的要求确保招聘流程符合中国隐私法律的要求。我们强烈建议您在设计合规流程前，先就相关事宜向您的法律顾问咨询。

Avature的卓越标准来自我们对保持 ISO、SOC 1 和 SOC 2 认证的承诺。Avature云计算通过国内的运营商中立主机代管数据中心运行，我们为客户提供全面的服务并配备经验丰富的本地专家团队。

随着《个人信息保护法》的生效，如果您的法律顾问建议您重新配置您的

系统，请联系您的销售代表，我们的顾问将根据您的指示重新配置。欲了解更多资讯，请联系您的Avature代表或发送邮件至**sales@avature.net**。

“在Avature，我们有丰富的与大型、流程复杂的跨国企业合作的经验，所以这不是我们第一次协助客户遵守新的隐私法规。我们看到，不同市场的法规有不同的变化。我相信，我们的可定制平台将使客户能够适应这些变化，同时让客户的招聘计划保持一如既往的竞争力。”

Manuel Sevilla
数据隐私保护官

附录

GDPR对比《个人信息保护法》

虽然《个人信息保护法》在许多方面与GDPR相似，但它规定了一些与GDPR不同的实质性义务，而且GDPR中有一些义务没有包括在《个人信息保护法》中。在下文中，我们会重点比较这些差异。

关键条款

《个人信息保护法》和GDPR对 “个人信息” 和 “个人信息的处理” 有类似的定义。敏感个人信息在《个人信息保护法》中被描述为

“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息”。（第二十八条）

请注意，相对于GDPR提供的符合敏感信息的封闭式清单，《个人信息保护法》是一个开放式清单，可供解读。

根据《个人信息保护法》，匿名化处理后的个人信息不被视为个人信息。在这里，“匿名化” 指的是个人信息经过处理无法识别特定自然人且不能以任何方式复原的过程（第四条和第七十三条）。

《个人信息保护法》使用 “受托人” 一词来指代GDPR所定义的 “数据处理者”。GDPR中定义的 “数据控制者” 概念在《个人信息保护法》中被称为 “个人信息处理者”，指 “在个人信息处理活动中自主决定处理目的、处理方式的组织、个人”（第七十三条）。

适用范围

与GDPR类似，《个人信息保护法》将其适用范围扩大到在境外对中国境内自然人个人信息进行处理的某些情况（第三条）。与GDPR对境外控制者任命 “欧盟代表” 的要求一样，《个人信息保护法》也要求，受《个人信息保护法》约束的境外个人信息处理者应当在中国境内设立 “专门机构” 或者 “指定代表”（第五十三条）。

合法依据

与GDPR相同，《个人信息保护法》要求组织拥有合法依据来处理个人信息（第十三条）。然而，《个人信息保护法》并没有提供GDPR中的 “正当利益” 作为处理的合法依据。

关于 “同意”，《个人信息保护法》第十四条和第十五条的定义与GDPR的同意要求相一致 (即，必须是知情的、自愿作出的、由个人的明确行动表明的，并且同意后可以撤回) 。

请注意，《个人信息保护法》要求对某些处理活动进行单独同意，比如个人信息处理者(i)与其他个人信息处理者分享个人信息；(ii)公开披露个人信息；(iii)处理敏感个人信息；或(iv)将个人信息转移到境外 (第二十三、二十五、二十九和三十九条) 。

数据主体权利

根据GDPR和《个人信息保护法》，个人拥有某些权利，组织 (即 “数据控制者” 或 “个人信息处理者”) 必须维护这些权利。数据主体访问请求是个人提交请求以行使一项或多项上述权利的一种方式。根据GDPR，组织一般有30天时间来回应此类请求，而根据《个人信息保护法》，组织有15天的时间来回应。尽管《个人信息保护法》规定的个人信息权利与GDPR规定的权利基本相似，但《个人信息保护法》规定的这些权利在实践中如何解释和执行仍不确定：

GDPR规定的权利	《个人信息保护法》规定的权利
查阅权	✓
纠正/更正权	✓
删除权	✓
拒绝处理或限制处理个人信息的权利	✓
要求提供数据转移途径的权利	(在特定条件下)
脱离自动化决策权	✓
撤回同意权	✓
向监管机构提出投诉权	✓

需要注意的一个重要区别是，根据GDPR，每个数据主体都被明确授予在其权利受到侵犯时向监管机构提出投诉的权利，而根据《个人信息保护法》，如果个人信息处理者拒绝个人行使其权利的请求，个人有权对其提起诉讼 (第五十条) 。但是，任何组织或个人都可以向负责个人信息保护的监管机构提出投诉，以防止个人信息处理者开展任何非法活动 (第六十五条) 。

个人信息保护影响评估

《个人信息保护法》要求个人信息处理者事先进行个人信息保护影响评估，并将以下情形的处理情况记录至少保留三年（第五十五和五十六条）：

- 处理敏感个人信息。
- 利用个人信息进行自动化决策。
- 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息。
- 向境外提供个人信息。
- 其他对个人权益有重大影响的个人信息处理活动。

虽然GDPR中包含了类似的义务，即事先进行个人信息保护影响评估（数据保护影响评估或DPIA），但触发这种要求的处理活动是不同的。此外，《个人信息保护法》没有要求，在评估结果表明某些剩余风险无法整改的情况下，需要向监管机构咨询。

联系我们，了解更多信息

欲获取实现PIPL合规的更多资讯，
请联系您的Avature代表或访问我们的网站

www.avature.net

艾睿德
Avature