敏感个人信息的处理要点

作者：潘永建 | 杨迅 | 杨坚琪 | 黄文捷

数字经济方兴未艾，正在日益与互联网、人工智能、云计算等行业深度融合发展。数据是数字经济的重要支撑，已成为除土地、劳动力、资本和技术外的第五类“生产要素”。数据保护与规范亟需法律从个人信息与隐私保护、企业数据权益、国家安全与监管等维度作出系统性的制度安排。作为数据保护制度的基础法律，《个人信息保护法》和《数据安全法》的重要性毋庸置疑。2021 年 4 月 29 日，《个人信息保护法(草案二次审议稿)》《数据安全法(草案二次审议稿)》公布。从企业使用数据和合规遵从的视角，通力网安数据业务小组对审议稿作出系列解读，本文为第五篇《敏感个人信息的处理要点》。

相比于一般的个人信息，敏感个人信息一旦遭到泄露或滥用，可能对个人人身或财产安全造成更大的损害，因此敏感个人信息亦应受到更加严格的保护。正因如此，《个人信息保护法(草案二次审议稿)》(以下简称“**《二审稿》**”)设专节对于敏感个人信息及其处理规则作出了规定。本文试从《二审稿》的规定出发，梳理现行法律法规下不同行业下敏感个人信息的处理要点，并结合我们的执业经验就敏感个人信息的处理提供实务见解与建议。

一. 《二审稿》对敏感个人信息处理提出的要求

作为中国个人信息保护领域的首部综合性法律，基于现行个人信息保护要求和实践中的监管经验，《二审稿》对于敏感个人信息的处理提出了更高的要求。依据《二审稿》第二章第二节以及第五章规定，处理敏感个人信息应当同时满足下列条件:

1) 具有“特定的目的”和“充分的必要性”;
2) 基于个人同意处理敏感个人信息时，应当取得单独同意;

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

3) 处理敏感个人信息的告知事项，除一般个人信息相关告知事项以外，还包括处理敏感个人信息的必要性以及对个人的影响；以及

4) 对敏感个人信息处理活动进行事前的风险评估，并妥善保管风险评估报告和处理情况记录。

1. 充分的必要性

《民法典》和《网络安全法》均对个人信息处理提出了“正当、合法、必要”的原则性要求。但是《民法典》和《网络安全法》均未对处理敏感个人信息时的“充分的必要性”要求进行进一步解释。从文义解释的角度来看，“必要”原则指的是在处理个人信息时应限定于实现目的所需最少个人信息和对个人主体影响最低的方式。在这一方面，2019 年 11 月发布的《App 违法违规收集使用个人信息行为认定方法》(“**《违法违规认定方法》**”)将“收集的个人信息类型或打开的可收集个人信息权限与现有业务功能无关”、“收集个人信息的频度等超出业务功能实际需要”，“因用户不同意收集非必要个人信息或打开非必要权限，拒绝提供业务功能”，“要求用户一次性同意打开多个可收集个人信息的权限，用户不同意则无法使用”等行为认定为“*违反必要原则，收集与其提供服务无关的信息*”的违法行为。《违法违规认定方法》不仅仅从收集信息的类型这一层面进行“必要性”的认定，还从**处理频率**、**收集方式**等层面考虑，意味着除了收集个人信息的范围之外，“必要”原则亦对个人信息的处理行为进行限制。2021 年 5 月 1 日生效的《常见类型移动互联网应用程序必要个人信息范围规定》(以下简称**“《必要个人信息规定》”**)则进一步规定 39 类服务收集的“必要个人信息”的范围，同时《必要个人信息规定》亦对收集“非必要个人信息”的行为作出限制，不允许因用户不同意提供非必要个人信息而拒绝用户使用其基本功能服务。我们理解，《必要个人信息规定》亦遵循了《违法违规认定方法》的精神，从收集个人信息范围和处理个人信息行为两方面对“必要性”原则进行解释。在实践中，监管部门亦从“范围”和“行为”两方面进行考察，例如上海市通信管理局在 2021 年 2 月 25 日通报的一批侵害用户权益典型案例中，曾将“社交类 App 应用嵌入的 SDK 插件存在高频率收集读取手机状态和身份等个人隐私信息行为，收集个人信息的频度超出业务功能实际需要”认定为“违反必要原则，收集与其提供的服务无关的个人信息”的行为。

而关于如何理解“充分的必要性”以及其具体判断方法，欧洲数据保护专员公署(European Data Protection Supervisor，简称“EDPS”)2019 年发布的《关于评估限制隐私权和个人数据基本权利的措施必要性的指南》[1]可资借鉴 。依据上述指南的规定，在判断必要性时，首先应说明待议的个人信息处理行为如何能实现处理目的，再将待议方案与对个人信息主体权益侵害更小的替代方案进行比较，说明侵害更小的替代方案不能同样有效地实现个人信息处理目的，方可证明必要性的存在。

综上所述，虽然现行中国法律对“充分的必要性”并未进行进一步的解释，但是结合已有的法律规定和监管实践，我们理解在判断“充分的必要性”时不仅仅需要考虑收集个人信息的范围的“必要性”，处理个人信息行为的“必要性”亦需要进行考察。而《二审稿》提出处理敏感个人信息应

[1] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data

基于“充分的必要性”，则必然会对“必要”原则提出更高的要求，我们期待监管部门在此方面给予进一步的回应。

2. 单独同意

根据《二审稿》第 30 条要求，基于个人同意处理敏感个人信息的，个人信息处理者应当取得个人的单独同意。也就是说，在获取个人信息主体同意时，个人信息处理者应当首先区分一般个人信息与敏感个人信息，并就敏感个人信息处理获取个人单独同意。

但令人遗憾的是，《二审稿》仍然未能明确“单独同意”实现的具体方式，给组织和企业处理敏感个人信息带来不确定性。根据我们的观察，为尽可能地实现“单独同意”的要求，企业往往会采取下列一种或者多种策略:

1) 个人信息处理者在其公示的个人信息保护政策中，为敏感个人信息处理设置专门的章节;
2) 以弹窗方式单独显示敏感个人信息处理的目的、方式和范围，例如微信小程序多以弹窗方式向用户告知收集位置信息并获取用户同意;
3) 为敏感个人信息准备单独的协议，例如阿里云为其人脸分析服务准备了单独的《人脸识别服务协议》以向用户说明处理目的、方式和范围。

不过上述方式能否满足处理敏感个人信息的“单独同意”要求，仍然有待主管部门给予进一步的解释。

3. 额外的告知事项

《二审稿》第 17 条对处理个人信息的告知义务进行了原则性的规定，而第 31 条在此基础之上对“处理敏感个人信息”提出了额外的告知义务。依据第 31 条的要求，在处理敏感个人信息时，相关个人还应当知悉处理敏感个人信息的必要性以及对其个人的影响。

根据该等要求，我们理解个人信息处理者应当先内部梳理处理敏感个人信息的范围，并核实和记录处理个人敏感信息的“必要性”，以及对个人主体的影响(例如是否会导致特定服务不能实现或者导致服务的质量下降)，最后在对外公示的《个人信息保护政策》中向相关用户明示上述内容，并获取用户的单独同意。

二. 其他法律法规对敏感个人信息处理提出的要求

除《二审稿》之外，许多单行法律法规规定了各个行业和领域的敏感个人信息处理规则。常见的单行法律法规(并非全部)中对处理敏感个人信息提出的要求示例如下:

1. 网络交易信息

2021 年 5 月 1 日生效的《网络交易监督管理办法》(以下简称“**《管理办法》**”)对于网络交易信息的处理提出了特别的要求。

首先，《管理办法》第 13 条定义了网络交易环境下的“敏感信息”，包括(但不限于)个人生物特征、医疗健康、金融账户、个人行踪信息。尽管《管理办法》使用的措辞“敏感信息”不同于《二审稿》中的“敏感个人信息”，上述四类个人信息不仅符合《二审稿》和《信息安全技术 – 个人信息安全规范 (GB/T 35273-2020)下》(以下简称“**《个人信息安全规范》**”)对于“敏感个人信息”和“个人敏感信息”的定义，监管部门通常亦将其认定为敏感个人信息。

其次，《管理办法》明确了敏感信息获取“单独同意”的方式，即网络交易经营者收集、使用多种敏感信息，应就每一种敏感信息逐项取得消费者同意。值得注意的是，网络交易语境下对敏感个人信息的“单独同意”采取了较为严格的解释，值得网络交易经营者重视。

2. 消费者金融信息

《中国人民银行金融消费者权益保护实施办法》(以下简称“**《实施办法》**”)适用于金融机构处理消费者个人信息的情形。《实施办法》将银行和支付机构通过开展业务等途径处理的消费者信息称为消费者金融信息，并明确列举消费者金融信息包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息等信息。

《实施办法》关于告知的要求较《二审稿》的规定更为宽松。《实施办法》允许银行、支付机构通过格式条款而非单独的弹窗向消费者告知收集消费者金融信息的目的、方式、内容和使用范围，但要求银行、支付机构以显著方式提示同意的可能后果。同时，针对目前金融消费者知情权利没有得到充分保护的现状，《实施办法》亦对收集消费者金融信息的方式提出特殊要求，例如“显著告知”、“业务关联”和“不得强制收集消费者金融信息”等要求。

值得注意的是，《个人信息保护法(草案)(一审稿)》规定，法律、行政法规规定处理敏感个人信息作出更严格限制的，从其规定。《二审稿》将“严格”二字删去，将上一句改为“法律、行政法规对处理敏感个人信息规定作出其他限制的，从其规定”。《二审稿》的修改并未明确敏感个人信息保护的一般法和特别法的法律适用规则。其他法律或行政法规就同一敏感个人信息处理事项(例如向个人告知的方式)作出比《二审稿》更为宽松的规定时，究竟应适用《二审稿》的规定还是其他法律、行政法规的规定，答案尚不明确。鉴于《实施办法》关于告知的要求较《二审稿》的规定更为宽松，并且从法律效力位阶的角度来看《实施办法》并不属于法律或行政法规，因此，如果《个人信息保护法》中关于敏感个人信息处理的法律适用的规定按照《二审稿》第 32 条的现状发布，银行、支付机构就消费者金融信息处理相关事项的告知方式是否仍然适用《实施办法》下的规定，仍有待主管部门给出进一步的解释。

3. 人类遗传资源信息

《人类遗传资源管理条例》(以下简称"**《管理条例》**")规范在中国境内进行的人类遗传资源采集、保藏、利用和对外提供等活动。其中，"人类遗传资源"包括"人类遗传资源材料"和"人类遗传资源信息"。"人类遗传资源信息"，根据《管理条例》的规定，指的是"所有利用含有人体遗传物质的器官、组织、细胞等遗传材料产生的信息"。未经匿名化处理的人类遗传资源信息在一定的条件下能够识别特定自然人，或者在特定自然人已识别的情况下属于与自然人有关的信息，因此特定的人类遗传资源信息也属于"个人信息"的范畴。同时，此类人类遗传资源信息拥有"个人生物特征信息"的属性，因此能够作为《二审稿》下的"敏感个人信息"受到法律保护。

《管理条例》对于我国人类遗传资源信息的采集、保藏、利用、对外提供活动作出了严格规范，包括事前审批制度、对外资的限制、符合伦理原则等。人类遗传资源信息处理的主要要点如下:

1) 采集人类资源前，应当全面、完整、真实、准确地向人类遗传资源提供者告知采集目的、采集用途、采集人类遗传资源对健康可能产生的影响，取得人类遗传资源提供者的书面同意，保证提供者自愿参与和随时无条件退出的权利;
2) 保藏我国人类遗传资源，仅当科技部批准后方能实施;
3) 利用我国人类遗传资源开展国际合作科学研究，仅当科技部批准后方能实施;
4) 向外方单位提供人类遗传资源信息能影响我国公众健康、国家安全和社会公共利益的，应当事先通过科技部的安全审查。将人类遗传资源信息向外方单位提供或开放使用，应向科技部备案并提交信息备份;
5) 禁止外方单位在我国境内采集、保藏我国人类遗传资源、向境外提供我国人类遗传资源。

4. 个人生物识别信息

个人生物识别信息目前还没有法律层面的明确定义。依据《个人信息安全规范》的规定，常见的个人生物识别信息包括人脸识别信息、基因信息、指纹信息、声纹信息等。《民法典》第 1034 条明确将生物识别信息列入个人信息的范畴，而《个人信息安全规范》的附录 B 亦将个人生物识别信息列为个人敏感信息。个人生物识别信息的唯一性使得此类信息一旦泄露无法通过修改的方式弥补，将给个人造成不可逆转和难以消除的侵害，因此有必要专门针对个人生物识别信息进行规范。

《个人信息安全规范》对个人生物识别信息这类敏感个人信息在存储、披露环节提出了特殊要求，主要处理要点包括:

1) 个人生物识别信息与个人身份信息分开存储;
2) 原则上不存储原始的个人生物识别信息，而应尽可能采取其他对个人权益侵害更小的替代措施，例如仅存储摘要信息、利用个人生物识别信息完成认证后删除原始图像;
3) 不得公开披露个人生物识别信息。

三. 敏感个人信息处理规则对企业的影响

随着数字化进程的加速，越来越多的行业开始需要处理敏感个人信息。例如，人脸信息等个人生物信息在当今社会被广泛应用于识别和认证自然人的身份，因此包括 App 运营者在内收集使用人脸信息的企业，都属于敏感个人信息的处理者。再如医疗健康领域，医疗健康类敏感个人信息的处理则涉及医疗机构、医药和医疗器械企业、接受委托处理医疗健康信息的 CRO 等第三方机构、互联网医院、健康医疗信息服务平台等多方主体。人脸识别、医疗健康、金融、网络交易、人类遗传资源等行业均属于敏感个人信息处理活动受到强监管的重点行业。

敏感个人信息本身的特殊性决定了此类信息处理存在特殊限制，因此敏感个人信息处理者更应谨慎处理敏感个人信息，避免承担更加严重的违法责任。例如，2017 年颁布的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》将非法获取、出售、提供行踪轨迹信息、通信内容、征信信息、财产信息等敏感个人信息的行为规定为侵犯公民个人信息罪的“严重情节”。

《二审稿》的出台为敏感个人信息重点企业就如何合规处理敏感个人信息提出了若干启示。我们建议大量处理敏感个人信息的企业提前采取下列合规措施，以满足将要适用的合规要求:

1) 识别并判断企业日常业务中收集处理的敏感个人信息种类和数量，明确合规义务范围;
2) 重新审视敏感个人信息保护相关规则，梳理适用于企业的敏感个人信息处理规则;
3) 根据适用的处理规则与合规要点，审视现有的敏感个人信息合规实践是否与法律要求的一致;
4) 对敏感个人信息处理活动在事前进行风险评估，并妥善保管风险评估报告和处理情况记录。

除《二审稿》《个人信息安全规范》中对于敏感个人信息的特殊规定以外，我们还重点提示企业应注意满足特定行业领域法律法规的要求，如我们在前文中提及的网络交易信息、消费者金融信息、人类遗传资源信息等。为读者参考之便，此处我们将敏感个人信息处理的主要要点总结如下:

敏感个人信息种类	处理要点
一般的敏感个人信息	具有“特定的目的”和“充分的必要性”
	基于个人同意处理敏感个人信息时，应当取得单独同意
	应向个人额外告知处理敏感个人信息的必要性以及对个人的影响
	对敏感个人信息处理活动在事前进行风险评估，并妥善保管风险评估报告和处理情况记录
网络交易信息	个人生物特征、医疗健康、金融账户、个人行踪信息等信息属于“敏感信息”
	应就每一种敏感信息逐项取得消费者同意
消费者金融信息	以显著方式向消费者提示同意收集消费者金融信息的可能后果
	不得收集与业务无关的消费者金融信息
	不得采取不正当方式收集消费者金融信息
	不得变相强制收集消费者金融信息

	不得以金融消费者不同意处理其金融信息为由拒绝提供金融产品或者服务，但处理其金融信息属于提供金融产品或者服务所必需的除外	
	若金融消费者不能或者拒绝提供银行、支付机构为履行反洗钱义务必须收集使用的消费者金融信息，银行、支付机构可以对金融消费者采取限制性措施，甚至拒绝向金融消费者提供金融产品或服务	
人类遗传资源信息	采集	全面、完整、真实、准确地向人类遗传资源提供者告知采集目的、采集用途、采集人类遗传资源对健康可能产生的影响
		取得人类遗传资源提供者的书面同意
		保证提供者自愿参与/随时无条件退出权利
		采集我国重要遗传家系等人类遗传资源的，应经科技部事前审批
		禁止外方单位在我国境内采集我国人类遗传资源
	保藏	应经科技部事前审批
		禁止外方单位保藏我国人类遗传资源
	利用	外方单位不得单独利用我国人类遗传资源开展科学研究活动，必须采取与中方单位合作的方式进行
		利用我国人类遗传资源开展国际合作科学研究，应经科技部事前审批
		为获得药品或医疗器械上市许可而利用我国人类遗传资源开展国际合作临床试验且不涉及人类遗传资源材料出境的，应向科技部备案
	对外提供	向外方单位提供人类遗传资源信息能影响我国公众健康、国家安全和社会公共利益的，应当事先通过科技部的安全审查
		将人类遗传资源信息向外方单位提供或开放使用，应向科技部备案并提交信息备份
		禁止外方单位向境外提供我国人类遗传资源
个人生物识别信息	与个人身份信息分开存储	
	原则上不存储原始的个人生物识别信息，而应尽可能采取其他对个人权益侵害更小的替代措施	
	不得公开披露个人生物识别信息	

敏感个人信息处理要点总结

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野