社会科学与教育 2026年第1期
ISSN: 3079-4420

商业银行个人敏感信息处理中最小必要原则的适用研究

高凡迪
中国邮政储蓄银行，北京，中国

【摘要】当前，我国有关个人信息保护的法律法规就个人信息处理中“最小必要原则”做出了框架性的规定，但缺乏对于各行业的具体指导。国内学术界对于个人信息保护理论在整体上的研究较多，但缺乏对于商业银行在该原则适用方面的专项研究。本文从商业银行实践入手，重点阐述了商业银行在个人客户敏感信息处理等方面的现状，论述了商业银行应用个人敏感信息的合理范围；阐述了现行法律法规与商业银行实际需求的矛盾。从平衡个人、商业银行和社会等多方利益的角度出发提出建议：一是在敏感信息分类评估方面，本文创新性地提出应用“预设场景法”来提前对个人敏感信息进行细化分类，尽可能把敏感信息进行量化评级。二是建议相关机构及商业银行制定关于银行处理个人敏感信息的最小必要性审查操作规范，并形成相关的评估机制。三是建议避免因过度保护个人客户信息，导致他人、商业银行或社会整体利益被侵害。就学界及实务界的代表性观点进行了比较和分析，较为充分的论述了完善建议。

【关键词】商业银行；个人敏感信息；最小必要原则

1.引言

伴随金融科技的发展，越来越多的商业银行运用个人客户敏感信息进行大数据分析，并应用于客户风险管理和营销过程中。目前，国内学界对于“最小必要原则”在商业银行个人敏感信息处理中的适用研究还比较少。本文结合当前国内银行业实际情况，对于该问题进行深入研究。

在理论方面，研究最小必要原则在商业银行个人客户敏感信息处理中的适用问题，对于完善银行领域的个人信息保护理论，为商业银行的个人客户信息保护和利用提供正当性依据均具有积极的作用。与此同时，银行领域的个人信息保护理论研究也将进一步丰富整体个人信息保护理论体系，为个人信息保护法律适用提供理论依据与参考。其实践价值在于，有利于个人信息保护的相关法律法规在银行领域的实际应用。

目前，国内对于个人敏感信息处理的最小必要原则有一些研究，但缺乏对该原则在商业银领域适用问题的相关研究。本文主要研究：在大数据背景下，商业银行在处理个人客户敏感信息时最小必要原则的适用问题。探讨相关场景下最小必要原则适用的解决方案，探讨如何有效平衡个人、商业银行、社会之间的利益。

本论文围绕“最小必要原则”展开讨论，结合国内外相关法律规制及理论，并结合相关案例，分析商业银行个人客户信息处理中“最小必要”原则的适用问题。相关研究方法拟采用“文献分析法”、“实证研究法”、“比较考察法”等。

2.银行处理个人敏感信息的现状

2.1 敏感信息的界定

我国《个人信息保护法》第 28 条规定了个人敏感信息的内涵：先是总体阐述敏感信息的特点，后又加上部分列举信息。这样的规定覆盖面比较全面，但在实践中这样的规定还需要解决一些问题：一是法律评价标准存在开放性、不确定性；二是在大数据及相关科技驱动下个人敏感信息的判定问题；三是从信息主体、信息处理方、国家（社会）不同角度判断标准不统一。

国内学者对敏感信息认定有不同观点：有学者认为，对于个人信息是否属于敏感信息的判断依据，应基于相关法律的标准进行判定，也可以结合场景因素来综合判断[1]。也有学者认为，应严格管理个人敏感信息，“在原则上禁止处理”，即无法律明确规定的除外事由的均不得处理，且“对于不同程度的个人敏感信息应当提供不同等级的防护举措”[2]。还有学者认为，使用个人敏感信息应受特定目的和充分必要性的约束；且始终围绕保护信息主体人格权益对于使用场景的合理性进行严格判断，“防止宽泛适用导致制度的滥用”[3]。有学者认为，我国对于敏感个人信息的规定缺乏动态的选择标准，应通过综合考虑各相关主体、信息的性质、信息的处理目的等多方面因素，动态界定敏感个人信息，这不仅利于切合实际的

标准建立，更有助于司法实践的科学合理开展[4]。笔者认为，在合理判定敏感个人信息时，也应当注意过度保护个人敏感信息的危害性。例如，曾有一个患精神疾病的人员因不能正常控制自己的金融行为，到很多银行开通信用卡并透支消费，导致其父母（监护人）经济上不堪重负并致信至央行及各大商业银行，主动透露其子的姓名、身份证号等信息，要求银行不给这个患病人员开通信用卡。因此，如果这种影响正常金融活动的个人敏感信息不被透露，就会给他人、银行，甚至社会带来不必要的负面影响。

国际上对于敏感信息解释有：1970 年，德国黑森邦《个人信息保护法》出现了敏感数据相关规定。1981 年，欧洲委员会通过《个人数据自动化处理中的个人保护公约》（简称“《108 号公约》”）。该公约第 6 条规定，有关种族、政治观点、宗教或其他信仰、健康或性生活的个人资料，除非法律提供适当保障，否则不得自动处理。欧洲联盟于 2018 年 5 月颁布了《通用数据保护条例》（简称 GDPR）。GDPR 第 9 条详细列举了基因资料、生理学辨识资料等敏感的个人资讯类型，以及与个人性取向相关的资料与自然人健康相关的资料。由于敏感个人信息的评价存在不易清晰判断，新类型的敏感个人信息可能会不断出现，因此归类标准存在争议。美国虽然没有统一界定敏感个人信息，但是对一些敏感个人信息在相关的、单独的单行立法中做了专门的规定。

目前，国内法律对于个人敏感信息有了一个框架性的规范并列举了一些重要的敏感信息，如何使敏感信息判定融入场景化信息，目前这种判定还处于较为浅层次的应用。笔者认为对于具体行业或场景的敏感个人信息仍需要进一步的细化研究，以下对商业银行收集个人敏感信息的范围进行阐述。

2.2 银行处理个人敏感信息的范围

商业银行收集个人客户信息主要用于客户业务办理、风险控制和业务拓展等方面，主要包括以下几个类别：身份识别信息、交易及信用信息[5]、社会公共记录、经个人同意的其他信息等。在《征信业务管理办法》第 3 条规定：“信用信息，是指依法采集，为金融等活动提供服务，用于识别判断企业和个人信用状况的基本信息、借贷信息、其他相关信息，以及基于前述信息形成的分析评价信息”[6]。

根据《个人信息保护法》对于个人敏感信息的规定，并参考人民银行 2013 年 1 月发布的《征信业管理条例》相关规定，商业银行应用的个人敏感信息主要包括以下几种类型：

（1）生物识别。例如，面部识别图像和特征信息等。

（2）行踪轨迹。例如，个人位置信息[7]等。

（3）收入和资产信息。例如，各类家庭收入，如薪金收入、经营性收入、租金收入等；各类家庭资产信息，如房屋、车辆等各项实物资产、存款、理财、国债、基金、保险、股票等各项金融资产。

（4）交易信息：例如，交易流水等。

（5）图像、视频信息。例如，个人客户签约和业务受理相关图像和视频信息等。

（6）其他敏感信息。例如，不满十四周岁未成年人的个人信息、司法、纳税、发票、社保、公积金、民政、物流等信息。

值得一提的是，随着大数据科技手段的应用，银行应用个人敏感信息的范围也在不断扩大，如上面提到的生物识别信息、银行以外的客户交易信息、其他银行外部的风险相关信息，包括司法、税务、发票、社保、公积金、民政、物流、位置信息等。但这些敏感信息的收集也存在一些争议，尤其在手机 App 上过度收集客户敏感信息。例如，2021 年 11 月，工业和信息化部发布了关于 App 违规问题的通报[8]，指出辽宁振兴银行等银行违反相关法律法规处理客户敏感信息。此前，光大银行、平安银行、招商银行等多家银行的 App 在收集客户敏感信息时也被通报。近期，笔者登录招商银行 App 申请信用卡时，被强制要求一键勾选同意《个人资信信息授权书》《敏感个人信息处理授权书》《个人信息共享授权书》及信用卡领用合约等多个文件，要求共享个人客户敏感信息，并同意接收其主动营销信息，否则不能申请信用卡。

2.3 银行处理个人敏感信息的授权

银行业是被强监管的行业，商业银行在收集个人敏感信息时一般会严格按照法律法规的要求进行，在征得个人客户同意的前提下收集相关信息。目前商业银行对于个人敏感信息的授权方式包括概括式授权和单独授权。概括式授权是指商业银行在与客户签订的协议中对于敏感信息进行概括性的描述，比如仅说明敏感信息的类别。单独授权是指商业银行在与客户签订的协议中对于敏感信息进行明确说明。关于敏感信息的收集方式，商业银行可以通过人工收集相关信息，也可以通过手机等

渠道收集客户相关信息。

3.个人敏感信息与特定目的相关性

根据《个人信息保护法》第 28 条，“只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下”[9]，商业银行方可处理敏感个人信息。因此，商业银行不宜采用概括的方式来论证敏感个人信息处理的合法性，而应当具体收集梳理敏感个人信息和具体的业务场景，确保所收集的敏感个人信息都具备相对应的特定的处理目的[10]。但有些银行的授权没有明确特定的处理目的。例如工商银行，笔者在该行 App 上申请信用卡时，看到该行要求信用卡客户共享部分敏感信息时处理目的不明确：“本人授权：中国工商银行可根据不同的信息处理目的，在依法合规的前提下，自行或委托有关单位处理本人账户信息、位置信息。”在这种场景下，客户就不能清晰地判断是否应该给相关银行授权。

以下对商业银行应用不同类别的个人敏感信息及银行特定目的之间相关性进行探讨。

第一，生物识别信息。随着信息技术、安全认证技术及生物特征技术的发展，又因生物特征技术在安全方面及客户感受等方面具有比以往人工方式突出的优势[11]，不少银行将开户、贷款、转账、支付等业务与生物识别技术相结合，近年来在银行领域获得迅速而广泛应用。国内多家商业银行在从原来的指纹识别发展为现在的虹膜识别、人脸识别、指静脉识别、多模态识别。从安全性和效益性方面考量，生物识别信息大大促进了商业银行安全性和效益性的提高，与商业银行提高经营质效直接相关。例如，招商银行在信用卡客户敏感信息授权文件上有提及此类敏感信息。

第二，行踪轨迹信息。商业银行在一些特别的业务领域需要了解个人客户的位置信息。从银行的安全性和效益性方面考量，使用这类信息可以促进银行某些业务经营的发展。但由于这类信息与人身安全等联系紧密，属于敏感度较高的信息。银行应判断何种业务场景有必要使用此类信息；另外，银行获取的信息也不是个人客户的具体位置，而是在一定空间和时间范围内的区间值，比如几公里以内，停留多长时间等。行踪轨迹作为高敏感信息，银行应该严格控制使用场景和知悉范围。例如，工商银行、招商银行在信用卡客户敏感信息授权文件上都有提及相关信息。

第三，收入和资产信息。各类家庭收入、资产信息是高度敏感的信息，但也是商业银行判断应该给客户多少授信的必要信息，从银行经营角度考虑是必要的。例如，招商银行在信用卡客户敏感信息授权文件上有提及这类信息。

第四，交易信息。这里的交易信息指的是收集客户在商业银行以外的客户交易信息。这些信息蕴含着客户的资金流向和资金量等高度敏感信息，对于银行客户行为分析有着重要的作用，能够有效帮助银行开展风险防控和业务拓展，是与银行经营密切相关一类数据。

第五，图像、视频信息。例如，个人客户签约和业务受理相关图像和视频信息等。这类信息是做相关业务佐证用的，可以作为办理业务的证明。这与银行经营密切相关，能够较好地保证银行业务开展的真实性。

第六，其他敏感信息。例如，不满十四周岁未成年人的个人信息、司法、纳税、发票、社保、公积金、民政、物流等信息。这些信息有助于银行更全面地把握客户风险信息，做出更为准确的判断。此类敏感信息在招商银行信用卡客户敏感信息授权文件上有提及。

目前，大多数商业银行 App 收集个人客户敏感信息授权都是通过一个整体的授权书，例如工商银行、建设银行、招商银行等，但《个人信息保护法》第 29 条要求“取得个人敏感信息应取得个人单独同意”，上述获取个人敏感信息授权的方式可能不符合相关法律要求[12]。

《商业银行法》第 4 条规定了商业银行的经营原则包括“安全性”、“效益性”。银行作为国家经济的重要组成部分，在保证其自身及整体社会安全的前提下，追求效益最优是合法、合理的。一般而言，银行收集个人信息是办理具体业务，比如某类个人贷款、信用卡。同时，收集个人敏感信息是银行判断个人客户整体信用情况的重要信息，收集信息的目的是既要保证银行的安全性和效益性，又要追求社会效益，因此银行收集的个人信息可能还会应用于银行的整体风险管理和交叉营销等领域。例如，某商业银行通过不同维度的数据交叉验证、对客户精准画像，选择符合要求的客户；提前排除问题客户，实现全行客户贷前准入阶段风险底线的统一[13]。这类对于客户整体信用情况的分析也应当属于特定目的范畴。

4.适用中存在的问题

4.1 严格适用最小化子原则的问题

商业银行收集个人客户敏感信息与其自身经营目标紧密相关，但严格适用最小化子原

则，存在着诸多现实困难。

第一，严格适用最小化原则，可能限制商业银行合理应用个人敏感信息的范围。当前，我国进入新发展阶段，受疫情冲击、经济下行压力加大，债务违约风险突出，互联网贷款业务资产质量压力较大。与此同时，信用风险日益呈现出隐蔽性、复杂性、突发性等新型特征。而传统的风险管理模式存在风险识别不全面、风险提示不及时的挑战，严重制约商业银行信用风险防控质效。由于缺乏对于客户自身风险和关联风险的识别与实时监测，使得银行的风险管理模式较为被动；对于个人客户全貌和潜在关系仍缺乏深入挖掘，在贷中评分和贷后监控力度较弱，导致风险提示滞后；不能提前发现客户风险变化或及时采取风控措施。在此形势下，大数据模型和智能化风控在银行风险监控中发挥越来越重要的作用，商业银行应用个人敏感信息的范围也逐渐扩大，有些原来办理业务不需要的信息，现在变得必不可少。比如，生物识别信息中的虹膜识别、人脸识别、指静脉识别、行踪轨迹信息等，如果严格适用最小必要原则，不应用这些信息，仍然延用银行过去办理业务的模式，会大幅降低业务办理的效率和风险控制的精准度[14]。笔者认为，在合理判定敏感个人信息时，也应当注意过度保护个人敏感信息的危害性。例如，曾经有患精神疾病的人员，因不能很好地控制自己的行为，到很多银行开通信用卡并透支消费，导致其父母（监护人）在经济上不堪重负并致信至央行及各大商业银行，主动透露其子的姓名、身份证号等信息，要求银行不给这个人员开通信用卡。类似这种影响正常金融活动的个人敏感信息不被透露，就会给其家人、银行，甚至社会带来不必要的负面影响。

第二，严格适用最小化原则，可能阻碍商业银行大数据风险管理技术的发展。我国实施大数据战略，鼓励数据开发利用和数据安全等领域的技术推广和商业创新（《数据安全法》第 14 条、第 16 条）[15]。机器学习必须在足够大的数据量基础上才能实现。严格适用最小必要原则，可能会对数据的大量积累和长期保存不利。另外，大数据分析方法有时候不能预设场景，这种不确定性可能在收集个人客户信息时与最小化原则产生矛盾。

第三，严格适用最小化原则，不能适应银行全品类业务线上化发展的需要。在商业银行数字化转型过程中，通过手机渠道开展银行业务已成为常态，从业务层面而言，银行授信类业务要从手机 App 收集的个人客户必要信息与人工收集的信息应一致。但现行的一些法律制度对于相关收集范围做了严格的规定，不能满足银行正常的信贷业务开展。例如，在《常见类型移动互联网应用程序必要个人信息范围》中规定的“手机银行类”、“网络借贷类”必要个人信息仅包括个人的基本信息和银行卡号，不包括个人的其他信用相关的信息，不能够为银行授信业务提供合理的数据支撑。上述规定限制了银行通过手机 App 开展授信等业务的信息收集的正常需求。大部分商业银行 App 在信贷类业务中的信息收集范围都包括个人信用相关的多类信息（包括个人敏感信息）。例如，招商银行 App、平安银行的 App。

4.2 合比例子原则的适用问题

《个人信息保护法》第 53 条规定：信息处理者对个人敏感信息处理前应当做个人信息保护影响评估。目前商业银行在实践中根据中国人民银行发布的数据安全分级指南在数据管理中对个人信息进行分类分级，但缺乏对个人敏感信息实际影响评估，主要是因为行业内缺乏统一的个人敏感信息归类评判标准、场景化的实际评估方法。简言之，商业银行在个人敏感信息使用中，合比例性原则还没有一个量化的落实依据和方法。

5.解决方案

从上述分析可以看出，商业银行认为有必要收集的个人敏感信息，一些法律法规及个人客户并不认同，这就要结合具体场景分析，平衡国家（社会）、商业银行和个人客户多方利益。

5.1 国外经验借鉴

首先，关于敏感数据的界定方法：《108 号公约》之后个人敏感信息逐步被越来越多的国家立法承认，随着适用场景的不同及科技的发展，出现了对个人敏感信息的不同界定方法，主要包括：

一是“分类列举法”：在确定敏感信息范围方面，目前大多数国家（地区）的立法主要是采用分类列举法。这种方法的隐含条件是这类敏感信息一旦被泄露，有很大的可能性会对信息主体产生严重的负面影响或伤害。这种方法可以明确地将个人敏感信息的种类及内容列举出来。因此这种方法可以节省信息处理者的论证时间，也可以为信息主体提供可靠的法律保证，在司法实践方面也较容易操作。但这种方法在确定敏感信息范围方面还是有缺陷的。首先，敏感信息不是一成不变的，随着

社会的发展、科技的进步，会增加原来没有的信息类型，像个人的 IP 地址等，还有人们观念的改变也会改变敏感信息的范畴。其次，非敏感信息与其他信息结合也会产生新的敏感信息。简言之，敏感信息的范围是随着时代的发展而变化的，应该客观判断[16]。以欧盟立法为例，随着时代的变化，列举敏感信息在立法中不断调整在一定程度上影响了法律的稳定性。

二是“场景判定法”：面对敏感信息分类列举法中存在的不足，一些学者提出了“场景判定法”。他们提倡个人敏感信息的灵活性，不是预先设定哪些信息属于个人敏感信息，而是要看具体的信息处理场景[17]。由于“场景”包含多种因素，在每一种特定场景下即使是同一个人信息的敏感度可能会不同，因此须不断地重新评估信息的敏感度。实践表明，同样的个人信息，在一种场景下敏感，而在另一种场景下则未必敏感。“场景判定法”不同于分类列举法的思维，它否认了某些个人信息具有先天的特殊性，强调了由于信息处理的特定场景所决定的个人信息的敏感性[18]，而不是源于信息本身的性质或内容。“场景判定法”依据个案的具体情境进行判断，对分类列举法所具有的固定性和滞后性，提供了有益的补充。但是该方法也有其瑕疵，具体来说，“场景判定法”不考虑信息本身的特殊性，即只有在特定场景下才能确定某人的信息是否为敏感信息，这就使得个人敏感信息处理规则的防范功能难以有效发挥，而只能通过事后救济的方式来实现法律上对个人敏感信息的保护，这就存在着很大的不确定性。同时，敏感的、与场景无关的信息就没有被判断的依据了。

三是“目的判定法”：该判定法主张由信息处理的目的来决定个人信息是否具有敏感性，即只有当信息处理的目的是要揭示他人敏感信息时才归为敏感信息。“目的判定法”操作性较强，但它也有一定的局限性。因为它必须依靠先行确立的敏感信息类型或范围，否则根本无法进一步判断信息处理的目的是否旨在揭示敏感信息。

综合分析上述三种对于个人敏感信息的判定法，均有其优劣势。根据《个人信息保护法》第 55 条第 1 款要求，敏感个人信息的判定是事前进行影响评估的法定情形，并非依据评估结果判断该信息是否属于敏感信息[19]。因此，商业银行根据自身实际情况，可以选择“分类列举法”来提前综合判断何为个人敏感信息。“目的判定法”只有当信息处理的目的是为了揭示敏感信息时，才会被判定为敏感信息，而银行的处理目的不是为了揭示敏感信息，而是为了防范风险和增加效益，同时尽量保护个人客户敏感信息的安全，所以不适用“目的判定法”。“场景判定法”在特定场景发生后再进行场景分析，属于事后判定，不适用《个人信息保护法》第 55 条第 1 款要求。

其次，关于敏感信息判定的操作方法，欧盟的《通用数据保护条例》（GDPR）是最小必要原则直接的域外渊源。欧盟为保障数据安全设立专门执法机构：欧洲数据保护专员公署（EDPS）。EDPS 为有效落实《欧盟宪章》与《通用数据保护条例》，同时鉴于最小化原则属于平衡数据利用与保护的核心原则，具有规范数据处理活动的重要地位，分别于 2017 年和 2019 年发布最小化审查的操作规范，这些规范被用于评估个人数据处理活动拟采用的措施是否符合欧盟数据保护的法律。其中必要性审查是最小化审查的第一部分；未满足必要性审查的措施无需进入比例性审查[20]。

5.2 适合我国的解决方案

个人敏感信息范围的大小会直接影响银行获取相关信息的难易程度。因此,敏感信息范围的界定至关重要,敏感信息的范围越大,银行收集个人客户信息的难度越大；敏感信息的范围越小,银行收集个人客户信息的难度越小。鉴于我国银行业对个人敏感信息范围的界定方法还有待进一步完善，为客观、准确地划分个人敏感信息的范围和等级，笔者建议如下：

第一，根据《个人信息保护法》第 55 条第 1 款的事前评估要求，我国商业银行在判定敏感信息范围时，可以结合“分类列举法”和“预设场景法”来进行个人敏感信息的分类。本文创新性提出“预设场景法”对敏感信息进行分类：这主要是考虑到银行使用个人客户信息是分场景的，比如风险管理场景、营销场景等，再进一步细分可以按具体业务或产品划分场景，每一类场景下信息处理对个人客户的影响程度可能不同，根据预设场景可能对个人客户的影响程度进行敏感信息分类。“预设场景法”既可以弥补“分类列举法”欠缺灵活性的不足，又能满足《个人信息保护法》对于事前评估的要求。笔者建议尽可能把个人敏感信息进行量化评级[21]，便于进一步的量化评估工作。

第二，在敏感信息审查方面，建议我国政府有关部门和商业银行可以借鉴国际经验，

立足我国国情及商业银行特点，建立适应社会发展要求的个人敏感信息最小必要性审查的操作规范；与之相匹配的，对于必要性和合比例性进行规范审查。

目前，国内很多商业银行还没有对于个人敏感信息的处理和保护制定具体规定，商业银行对于个人敏感信息的审查还处在起步阶段。建议国内商业银行：一是结合自身业务特点和相关法律法规要求，建立个人敏感信息处理和保护的具体制度。二是对于银行个人客户敏感信息的判定制定具体的标准，并依据特定业务场景制定敏感信息的分类分级标准。三是在敏感信息审查方面，建议商业银行建立全流程审查机制，包括但不限于收集、加工、使用、存储、传输、提供、删除等环节（包括对系统中个人敏感信息的应用监控）。

表 1.某业务场景下某类个人客户信息的影响评估模型

主体类型	因素 1 的影响	因素 2 的影响	.....	因素 X 的影响	总体影响
个人	因素 1 的影响力评分*权重系数 1	因素 2 的影响力评分*权重系数 2	.....	因素 X 的影响力评分*权重系数 X	各因素影响加总
商业银行	因素 1 的影响力评分*权重系数 1	因素 2 的影响力评分*权重系数 2	.....	因素 X 的影响力评分*权重系数 X	各因素影响加总
社会	因素 1 的影响力评分*权重系数 1	因素 2 的影响力评分*权重系数 2	.....	因素 X 的影响力评分*权重系数 X	各因素影响加总

第三，在个人敏感信息处理中，应平衡个人、银行、社会等多方权益。这里所说的权益既包括经济利益，也包括非经济类权益，例如个人隐私权、安全权等。平衡上述三方权益，需要先分别考量上述三方在个人敏感信息处理中的受到的正、负面影响。这里可以引入量化评分的方法，来综合判断各类因素对于三方主体的影响（见表 1）。在此基础上，根据三方主体受到的综合影响情况（正负面影响、影响程度大小等）来进一步判断是否应当使用该敏感数据，在什么情况下使用该敏感数据，应采取何种保护措施等。这样可以避免因过度保护任意一方的利益，造成对其他两方的严重负面影响。

具体实施的初步设想：

当 3 类主体的“总体影响”全部为负时，建议在此业务场景下不使用该类个人敏感数据。

当 3 类主体的“总体影响”2 负 1 正时，建议在此业务场景下审慎使用该类个人敏感数据，加强相关保护措施。

当 3 类主体的“总体影响”2 正 1 负时，建议在此业务场景下适当使用该类个人敏感数据，适当增加保护措施。

当 3 类主体的“总体影响”全部为正时，鼓励在此业务场景下使用该类个人敏感数据，采取一般性保护措施。

参考文献

[1]王利明.敏感个人信息保护的基本问题：以《民法典》和《个人信息保护法》的解释为背景.当代法学，2022（1）：3，8-11.

[2]朱荣荣.“后民法典时代”个人敏感信息的法律保护.大连理工大学学报（社会科学版），2022，43（5）：109.

[3]李世刚，屈然.论敏感个人信息的合理使用.江苏社会科学，2022（6）：159.

[4]王苑.敏感个人信息的概念界定与要素判断——以《个人信息保护法》第 28 条为中心.载《环球法律评论》2022 （2）：85.

[5]顾男飞，张帆.利用与保护：基于信息可携权的个人信用信息采集机制.征信，2022（10）：47-48.

[6]人民银行：《征信业务管理办法》，http://www.gov.cn/zhengce/zhengceku/2021-10/01/content_5640685.htm。

[7]卢丹，王琦，王可，邵晓萌，韩佳琳.移动用户位置信息安全保护策略研究.技术与标准，2022（10）：94-95.

[8]工业和信息化部信息通信管理局：《关于 APP 超范围索取权限、过度收集用户个人信息等问题“回头看”的通报（2021 年第 11 批，总第 20 批）》，https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2021/art_1b4410dcdc9743edae30b6429bd76d22.html。

[9]中国法制出版社编：《个人信息小法典》，中国法制出版社，2021 年。

[10]刘新宇.中华人民共和国个人信息保护法重点解读与案例解析.中国法制出版社，

2021.
[11]吴彩霞.金融领域生物识别技术应用探析.金融理论与实践，2018（12）：61。
[12]刘新宇.中华人民共和国个人信息保护法重点解读与案例解析.中国法制出版社，2021 年。
[13]李爱娅.智慧风控在商业银行信贷领域的应用探索.农银学刊，2021（6）： 74.
[14]王苑.敏感个人信息的概念界定与要素判断——以《个人信息保护法》 第 28 条为中心.环球法律评论，2022（2）：85.
[15]严强.区块链+隐私计算：科技驱动数据安全体系建设.金融电子化，2021（7）：43.
[16]韩旭至.敏感个人信息的界定及其处理前提 ——以《个人信息保护法》第 28 条为中心.求是学刊，2022（5）：133.
[17]王利明.敏感个人信息保护的基本问题：以《民法典》和《个人信息保护法》的解释为背景.当代法学，2022（1）：9-11.
[18]孙清白.敏感个人信息保护的特殊制度逻辑及其规制策略.行政法学研究，2022（1），120.
[19]韩旭至.敏感个人信息的界定及其处理前提 ——以《个人信息保护法》第 28 条为中心.求是学刊，2022（5），134.
[20]金龙君，翟翌.论个人信息处理中最小必要原则的审查.北京理工大学学报（社会科学版），2022（6）：6-8.https://doi.org/10.15918/j.jbitss1009-3370.2022.0363.
[21]谢琳，王漩.我国个人敏感信息的内涵与外延.电子知识产权，2020（9）：12.