建筑工程信息共享机制与 GDPR 原则的适配性对比研究

邓晖[1]，徐伊雯[1]，李晓瑶[1]，邓逸川[1]，林佳瑞[2]

（1.华南理工大学 土木与交通学院，广东 广州 510641；
2.清华大学 土木工程系，北京 北京 100084）

摘　要：随着建筑信息模型（Building Information Modeling, BIM）等先进信息技术应用的不断深入，建设项目全生命周期各个阶段储存的工程信息体量迅猛增长。工程信息共享在提高工程建设效率的同时，亦引发从业者对数据安全问题的关注。欧盟出台的《通用数据保护条例》（General Data Protection Regulation, GDPR）是当前数据安全领域影响范围最广数据保护法规，得到国内外广泛关注。本文从工程信息安全指标、BIM 标准规范、BIM 平台相关软件三方面分析建筑工程信息安全机制与 GDPR 数据处理原则的适配性。结果表明，GDPR 数据处理原则与建筑工程信息安全机制适配性较好，对解决建设领域数据安全问题具有重要参考意义。为保障建筑工程数据安全，未来仍需在领域法规体系建设、第三方数据安全监管等方面加强探索与实践。

关键词：工程信息共享；GDPR；数据安全；BIM

中图分类号：F283　　**文献标识码：**A　　**文章编号：**

随着建筑信息模型（BIM）在建筑工程项目中的应用不断深入，工程信息得以在各利益相关方、阶段、专业之间沟通传递。BIM 模型在建设项目全生命周期的各个阶段均储存着大量信息，工程项目各相关方可在 BIM 模型中输入、获取、更新和修改工作所需的信息[1]。BIM 作为工程单一数据源，其信息由参与方分享。然而共享中数据的滥用会反作用降低原始分享者积极性，并带来信息安全隐患。如何规制建筑信息安全问题、识别 BIM 功能特性带来的风险、在不影响 BIM 使用的基础上开展信息数据安全保护具有紧迫性、重要性。本文将建筑工程信息共享机制定义为建筑工程各参与方在进行信息共享过程中所遵循的原则、行为规范及相应的技术手段。随着信息系统在建筑工程中的深度应用，建筑工程信息共享机制的设计成为制约各参与方合理分享及使用工程信息的重要因素。

目前已经有不少学者在技术层面开展建筑工程的信息共享的相关研究，但仍存在诸多局限与挑战，具体体现在建筑工程信息共享过程中的机制定义不明，无法准确把握所开发的技术的适用性。2018 年 5 月 25 日，《通用数据保护条例》（GDPR）在 28 个欧洲经济区国家统一实施生效，该条例成为全球数据保护领域影响范围最大、要求最全面、罚款金额上限最高的正式法律，并在个人信息安全保护领域树立了数据安全领域国际新标杆。因此，将 GDPR 引入工程信息安全管理具有可靠性与借鉴意义。本文将从建立建筑工程信息共享机制的视角，从 GDPR 所体现的关于信息共享的原则出发，从工程信息安全指标、BIM 标准规范和 BIM 平台软件三个方面研究 GDPR 原则在工程信息共享机制中的适配性，并基于上述分析总结工程信息共享问题、提出相应建议。

1 建筑工程信息共享及 GDPR 相关研究现状

BIM 等建筑信息化管理平台在降低工程管理成本、为工程相关方及时掌握工程信息提便利的同时，也对工程信息共享过程数据安全和利益相关方信息隐私权利带来挑战。项目工程信息应当如何采集、应用、储存、流转、保护、删除，如何更好地平衡效率与工程信息数据安全之间关系的问题亟待解决。

1.1 工程信息共享

手稿日期：2021-07-18
作者简介：邓晖（1969-），男，湖南人，副教授，博士，研究方向为智慧建造（Email: hdeng@scut.edu.cn）
基金项目：

信息在我国环境下有个人／企业、数据平台、政府等三个主要参与方，具体关系如图 1 所示。个人／企业是信息的产生者，个人／企业对于自身产生的信息拥有天然获取的权力。数据平台依靠为个人/企业提供服务，借助大数据、物联网等技术获取大量信息，并通过数据信息的分析应用进行盈利。政府出于公共管理的需要对所有信息有依法获取、管理的权力。

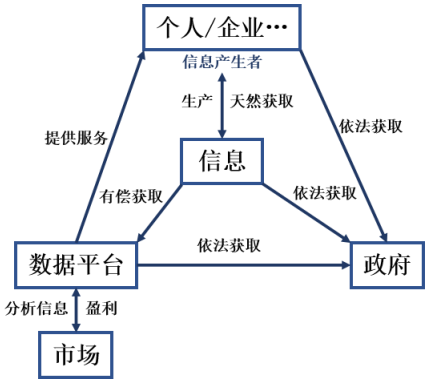

图 1 信息各参与方关系

对于工程行业而言，工程本身存在临时性、松散性的特征，工程信息具有体量庞大、形式多样、随时间变动、参与方复杂等特点。此外，随着信息科技的进步、信息化技术手段的应用使项目工程信息爆炸式增长，数据资源不断累积。张建平教授[2]认为 BIM 的本质是工程单一数据源，这意味着所有工程参与方均应将数据信息分享至 BIM 平台。如果没有合理的信息共享机制，会出现参与方对工程信息的滥用、误用，形成建筑工程信息安全隐患。此类问题的存在进一步反作用至信息的原始分享者，从而降低信息分享积极性；另一方面，工程信息所有权问题可能会变得更加复杂，信息泄露的责任问题难以界定。

目前已经有学者在技术层面开展建筑信息共享方面的研究，但从网络安全原则、分布式环境的特征、BIM 功能以及建筑项目的性质等角度来识别和评估 BIM 安全性的综合性研究仍处于缺乏状态，且目前存在 BIM 协同平台数据安全保护实践和技术应用程度较低、欠缺系统性等问题[3]。Singh 等人[4]引入了 BIM 安全性的概念，主张在 BIM 服务器的设计中需考虑保密性、完整性和可用性（CIA）等网络安全原则。Olatunji 等人[5]阐明了跨多个地理区域的 BIM 模型信息数据共享中网络安全漏洞可能导致的法律后果，并提出开发适当自定义安全策略的建议。Afsari 等人[6]总结了 BIM 信息共享过程中与安全相关的挑战和威胁，例如基于云计算的 BIM 平台中责任和信息所有权问题。Parn 等人[7]对建筑环境网络安全进行了研究，同时分析了黑客窃取建筑环境相关信息的动机。Zhang 等人[8]通过构建私有云/混合云环境，在保证数据所有权的同时通过数据虚拟集成实现数据共享。目前主要有四种常用的信息安全技术用以保护 BIM 信息安全：加密协议[3,9~11]、分布式数据库技术[12,13]、BIM 云[3]、区块链技术[3,14,15]，然而，学者们在开发相应的数据共享技术的同时，却往往忽视了技术的应用规则。如何应用所开发的技术实现建筑工程数据共享，保证各参与方的合法权益，不仅依靠于技术的进步，也依赖于合理的建筑工程信息共享机制。

综上所述，工程信息的共享不仅是节省建造成本的过程，更是建筑工程项目必不可少的生产要素。鉴于建筑工程项目的临时性、松散性以及 BIM 本身的多参与方、复杂庞大等特性，完善工程相关的数据共享机制，以规制各参与方的数据使用行为显得尤为重要。工程信息共享机制研究的核心问题在于：规制到何种程度才能有效保护数据主体的权利，却又不妨碍工程项目各相关方主体权利的实现及工程执行的效率。在此方面，GDPR 所呈现的基本原则具有重要的参考意义。

1.2 GDPR 及其基础内容

《通用数据保护条例》（以下简称 GDPR）的立法原则是权利与自由、处理正当性、最小侵害性[16]。条例规定保护自然人的个人数据保护权，承认自然人在其个人数据处理过程中获得保护是一项基本权利。表 1 所示为 GDPR 数据处理七大原则及相关解释说明。表 2 为 GDPR 对数据控制者和数据处理者主要义务的规定。

表 1 GDPR 数据处理七大原则

七大原则	相应解释
G1 坚持合法性、公平性和透明性原则	——
G2 坚持目的限制原则	即以特定、明确、合法的目的进行数据收集，同时个人数据后续的数据处理不得违反以上规定。
G3 坚持数据收集最小化原则	数据最小化即对个人数据的收集和处理应限制在完成所需工作必要的最小限度内。
G4 坚持准确性原则	即确保数据准确、处理的必要与及时，不准确的个人数据应及时删除或修正。

G5 坚持存储限制原则	储存限制是指允许数据主体为了实现公共利益、科学、历史研究或统计的目的，以可识别的方式存储数据，同时数据保存时间不得长于为达到个人数据处理目的所需的必要时间。
G6 坚持完整性和机密性原则	即要采取措施保证数据安全，防止其遭到破坏；
G7 坚持责任性原则又称（问责制）	即数据控制者或处理者对数据的管理和操作负有主体责任。

表 2 GDPR 对数据控制者、处理者的义务规定

两大义务	相应解释
1. 采取数据系统保护和默认保护	数据控制者应当采取一定技术、组织措施（如匿名化等）确保数据处理符合 GDPR 要求的同时又保护数据主体的权利。此外，在默认（by default）情形下，该技术和组织措施应保证对个人数据的处理应在最小必要的原则下进行且不得被不特定自然人访问。
2. 记录数据处理活动	数据控制者和处理者应当保存由其负责的数据处理活动的记录，该记录应当采取书面形式，必要时向监管机构提供。

对一切单独和结合起来足以识别特定自然人的信息的收集、记录、储存、共享等行为均可被认定为 GDPR 项下的“个人数据处理”，而工程信息共享过程中的数据互用同样包括信息的获取、记录、更新、储存、管理和共享等过程，因此 GDPR 所提出的原则具有一定的参考意义。此外，GDPR 对数据控制者、处理者的义务规定与工程信息数据相关的要求不谋而合。例如，我国现行 BIM 应用标准《建筑信息模型应用统一标准》中明确规定应采取技术措施保障模型数据信息安全，并且规定应详细记录模型所有权的状态，模型的创建者、审核者及更新者和相应时间等信息，并在模型交付时完整附上。

此外，GDPR 要求企业在内部建立完善的问责机制。一是创新性地要求企业设数据保护官（Data Protection Officer）, DPO；二是要求数据保护过程进行文档化管理[17]。因 GDPR 数据信息保护范围、规定的数据主体及使用者义务和权利、处理原则的合理性和适用性，在工程信息共享过程中同样可借鉴 GDPR 对于个人信息保护提出的解决方法。本文根据 GDPR 规定的范畴以及工程实践应用过程，例如工程信息安全指标、BIM 标准规范、BIM 平台相关软件，分析对比现有的工程实践与 GDPR 是否存在抵触条款、是否配适、是否有已经匹配的部分，为后续提出建筑工程的信息共享机制提供理论依据。

2 建筑工程信息安全与 GDPR 的配适性分析

本章将从工程信息安全指标、BIM 标准规范、BIM 平台相关软件三方面开展 GDPR 配适性研究，如图 2 所示。

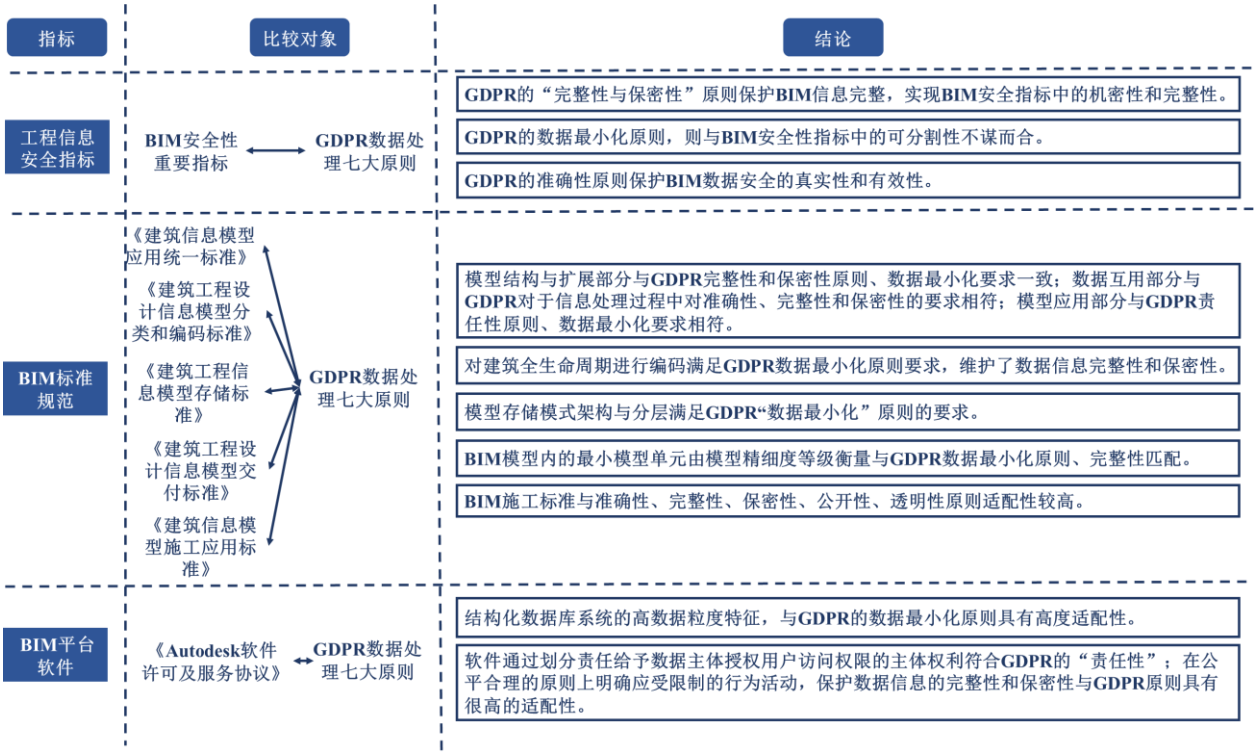

图 2 工程数据安全与 GDPR 配适应研究框架

2.1 工程信息安全指标的适配性

为保障 BIM 信息安全，需要考虑以下几个基本安全要求：数据主体的数据所有权、信息共享过程中的数据传输安全、模型信息数据的完整性与准确性。Das 等人[3]为了进一步明确 BIM 安全的主要研究对象，基于 BIM 的功能和用户需求采用文献综述法确定了七个 BIM 安全性具体组成部分：数据所有权、数据共享(查询/搜索)、BIM 模型的数据集成、信息工作流、数据安全(或静态数据安全)、网络安全、系统安全。如表 3 所示，根据网络安全原则与 BIM 安全标准得出上述七个具体安全组成部分中保障 BIM 安全性的指标：（1）机密性；（2）完整性；（3）有效性；（4）真实性；（5）可分割性。

表 3 BIM 安全性重要指标

BIM 安全性指标	指标定义
机密性	机密性是指为保护数据隐私，防止未经授权的用户访问或使用数据
完整性	完整性是指用户接收到的数据是完整、未被篡改的。
有效性	有效性是指确保被授权用户始终可以访问数据，并防止数据被恶意进程掩盖。
真实性	真实性是指确保数据的真实准确，确保数据被授权创建或认可，以及确保用户的真实性。
可分割性	可分割性是指将部分 BIM 模型/数据在信息共享过程中按数据粒度（可以共享、更新及加密的 BIM 模型信息的最小单元）进行划分，将划分后的 BIM 数据分发给不同的项目参与方，从而保护数据机密性和完整性。

通过对比可知，工程信息共享过程中的信息安全指标与 GDPR 数据处理过程中信息保护的原则具有很高的适配性，GDPR 的“完整性与保密性”原则能够很好地约束未经授权的用户修改传递中的数据，保护 BIM 信息完整，不被篡改，从而实现 BIM 安全指标中的机密性和完整性。

GDPR 的数据最小化原则，则与 BIM 安全性指标中的可分割性不谋而合，数据最小化原则要求将个人数据处理过程分解，尽可能缩短处理个人信息的时间以及减少参与方，从而保护个人信息隐私安全。BIM 信息在建设全生命周期过程中需要分享给不同项目参与方，且由于 BIM 模型构建过程中模型信息具备可分性和高数据粒度性，可以通过对 BIM 模型的部分访问和修改控制，从而实现保护工程信息安全的目的。

除此之外，GDPR 的准确性原则能够及时修正不准确信息，维护数据完整准确，保障数据真实有效，防止未授权用户访问数据，从而保护 BIM 数据安全的真实性和有效性。同时，以合理合法、公开透明的原则、目的限制原则、储存限制原则及问责制贯穿工程信息共享和数据交流全过程,在提高信息传递效率的同时兼顾信息安全，数据主体的数据所有权、信息共享过程中数据传输安全、模型信息数据的完整性与准确性均能得到保障。

2.2 BIM 标准规范的适配性

《建筑信息模型应用统一标准》是 2018 年 1 月 1 日开始实施的推荐性标准，因其在 BIM 标准领域的重要性，该标准与 GDPR 原则是否适配，很大程度上代表了基于 BIM 的工程数据共享的实践过程与 GDPR 原则的匹配度。

标准基本规定部分对 BIM 模型应用提出的基本要求包括模型应用应实现工程各相关方协同工作、信息共享，同时在应用过程中应采取措施保障信息安全。这与 GDPR 的数据主体应采取技术措施以保证数据信息的完整性和保密性要求一致。

模型结构与扩展部分提出了开放性、自定义的要求，这一要求能保证 BIM 模型数据完整性，同时也与 GDPR 完整性、保密性原则要求一致。该标准还提出了 BIM 模型应根据工程项目各任务要求逐步细化，增加模型数据也应该采用属性或属性集的扩展方式，这与 GDPR“数据最小化”原则要求一致。

数据互用部分要求建设工程全生命期各阶段、各项任务的 BIM 模型应用均明确模型数据交换的内容与格式，确保相关方均能获取、更新、管理信息，实现协同工作；数据部分要求保障工程信息共享过程中的数据分享透明性、数据信息准确性及完整性。《建筑信息模型应用统一标准》对工程信息共享过程中的数据具体内容有明确规定，对数据格式转换提出正确性、完整性的要求。这与 GDPR 对于信息处理过程中准确性、完整性和保密性的要求相符。标准同时规定了互用数据的内容应根据专业或者任务要求细化，并根据模型创建、使用和管理的需要进一步分类和编码，即 BIM 模型信息可分割性的体现,因此 GDPR“数据最小化”原则的具体要求对 BIM 模型信息数据共享有一定的参考意义。

模型应用部分规定各相关方应建立支持协同工作、数据共享的环境和条件，应具备完善的数据存储与维护机制，明确责任划分，为数据安全构建合理的环境与条件，这与 GDPR 责任性原则要求相符。这一部分还规定了在模型创建和使用过程中，应根据工程项目不同阶段、不同专业以及不同任务划分模型及子模型，并在模型使用过程中采用以下形式开展数据更新交换：从模型中提取出满足任务需求的数据形成子模型，在子模型上进行数据交流变更。这一要求在提高信息共享效率，提高协同工作效率的同时，也满足 GDPR“数据最小化”基本原则，在完成任务所需的最小限度内对信息数据进行收集和处理，为工程信息共享过程中的数据安全保护提供新思路。

表 4 《GBT 51212-2016 建筑信息模型应用统一标准》与 GDPR 原则对比分析

	G1	G2	G3	G4	G5	G6	G7
3.0.1	√					√	
3.0.4							
4.2.4			√				
4.3.2							
5.1.1	√			√		√	
5.1.2							
5.1.4							
5.2.1				√		√	
5.2.2			√			√	
5.2.3				√		√	
5.2.4							
5.3.1	√		√				
5.3.2	√					√	
5.3.3							
6.1.4						√	
6.1.5							
6.3.1			√				
6.3.4							
6.4.2			√				
6.4.4				√			√
6.5.3						√	√
6.5.4				√		√	√
6.2.3	√					√	

注：横坐标为 GDPR 七大原则，与表 1 对应简写；纵坐标为《GBT 51212-2016》对应条款编号。

《建筑工程设计信息模型分类和编码标准》对建筑全生命周期进行了编码，包括模型及信息、项目各相关方、各项任务均有相应的编码。为了实现建筑工程全生命期信息交换与共享，需要规范 BIM 模型中信息的分类和编码，从而推动 BIM 在建筑工程的应用和发展。将模型信息

进一步细化，既能提高工程信息共享效率，又能将模型信息数据隔离，各相关方利用 BIM 模型收集、完善、共享各自完成工作任务所需数据，是 BIM 安全性指标中可分割性的重要体现，满足 GDPR“数据最小化”原则的要求，同时使工程信息所有权划分更为明确，更大限度上防止未经授权的用户私自访问与之无关的工程信息，维护了数据信息完整性和保密性，各任务相关方独立工作也在一定程度上保护信息数据安全。

《建筑工程设计信息模型交付标准》主要对项目规划及设计阶段中 BIM 模型的命名规则、模型精细度、交付物等做了详细的要求。《标准》规定 BIM 模型内的最小模型单元由模型精细度等级衡量，这与 GDPR“数据最小化”原则的基本要求匹配。

表 5 《GB/T 51301-2018 建筑工程设计信息模型交付标准》与 GDPR 原则对比

	G1	G2	G3	G4	G5	G6	G7
4.2.2			√			√	

注：横坐标为 GDPR 七大原则，与表 1 对应简写；纵坐标为《GB/T 51301-2018》对应条款编号。

《建筑信息模型施工应用标准》规定了在施工过程中应用 BIM 的具体操作，以及交付施工模型信息的具体规定，《标准》中明确规定在模型信息传递共享过程中要保证数据完整性和安全性，及时记录变更信息，确保模型信息准确，这既符合 BIM 安全性指标中对完整性、机密性、有效性的要求，也与 GDPR 准确性、完整性、保密性、公开性、透明性原则适配性较高，《建筑信息模型施工应用标准》是《建筑信息模型应用统一标准》的细化，因此其与 GDPR 适配性也和《建筑信息模型应用统一标准》相似，在此不再赘述。

表 6 《GB/T 51235-2017 建筑信息模型施工应用标准》与 GDPR 原则对比

	G1	G2	G3	G4	G5	G6	G7
5.1.4				√		√	
5.2.5							
5.2.4				√			
5.3.1			√				

注：横坐标为 GDPR 七大原则，与表 1 对应简写；纵坐标为《GB/T 51235-2017》对应条款编号。

2.3 BIM 平台软件与 GDPR 的配适性研究

随着 BIM 应用的不断深化，工程项目全生命周期过程中的信息沟通和数据交流共享得以实现。为了更高效地存储、共享 BIM 信息数据，许多软件商都推出了 BIM 云平台。BIM 云平台在促进信息交流的同时，也带来不少信息安全争议。以云技术为基础的 BIM 云平台，可以分为 IaaS（基础设施服务）、PaaS（平台服务）、SaaS（软件服务）三个层面。相应的，基于 BIM 的工程信息共享也可划分为三个级别进行考量，分别是：非结构化文件系统、结构化文件系统以及结构化数据库系统[3]。随着 BIM 云平台软件的不断应用和发展，结构化数据库系统的高数据粒度特征，与 GDPR 的数据最小化原则具有高度适配性，能够确保数据的所有权，具备可分割性，能够维护 BIM 模型信息的机密性、完整性、有效性以及真实性。BIM 相关软件中，使用较多的设计建模软件有 Revit、AutoCAD、ArchiCAD、Navisworks 和 digital project 等。本文将以《Autodesk 软件许可及服务协议》为主要研究对象，该协议适用于全球 Autodesk 旗下所有软件，包括常用的 BIM 相关软件，对比该协议相关条款与 GDPR 基本原则的适用性，为 GDPR 对于 BIM 信息共享的参考作用提供参考依据。

《Autodesk 软件许可及服务协议》主要从许可、许可的禁止与限制、保留信息所有权规定、隐私和信息使用、有限担保及拒绝担保、警示、责任限制、期限和终止、一般规定、其他条款等十个方面展开。协议中规定了数据主体授权其他用户的权责范围，明确被授权的用户必须遵循《Autodesk 软件许可及服务协议》，才能正常使用软件，访问或修改数据信息，通过划分责任给予数据主体授权用户访问权限的主体权利，防止未经授权用户访问数据信息，从而确保数据安全，与 GDPR 的“责任性”有很高匹配度。

协议规定对于未经授权许可的信息访问或者修改活动应当给予限制或禁止，在公平合理的原则上明确应受限制的行为活动，保护数据信息的完整性和保密性；明确规定破解 Autodesk 技术保护措施的禁止行为，在维护数据准确性的同时确保了完整性和机密性，与 GDPR 原则具有很高适配性。

表 7 Autodesk 软件许可及服务协议

	G1	G2	G3	G4	G5	G6	G7
1.5							√
1.9					√		
2.1.1	√					√	
2.2.1				√		√	
2.2.2							
6.1				√		√	√
6.2.2				√		√	

6.3						√	

注：横坐标为 GDPR 七大原则，与表 1 对应简写；纵坐标为《Autodesk 软件许可及服务协议》对应条款编号。

通过表 4~表 7 分析可知，我国现行 BIM 标准中工程信息共享数据安全的相关规定，能够满足 GDPR 合法公平透明性、数据最小化、准确性、完整性和保密性等原则。同时，通过表 8 中所体现的 BIM 标准与 GDPR 原则的对比，可以发现现行 BIM 标准虽然与 GDPR 原则有较高的适配性，但在目的限制、存储限制、问责制原则的规制方面仍待加强。在数据收集和处理阶段，应当通过细化任务，将 BIM 模型信息分割为更小的模型单元，限制不同专业间的数据收集、处理目的，从而更好地保护数据安全不受侵害；此外，应当规定限制数据处理时间，明确数据主体与数据处理者的权利和义务，权责划分明确，进一步保护数据主体的信息安全。

表 8 BIM 标准与 GDPR 原则对比

	G1	G2	G3	G4	G5	G6	G7
《建筑信息模型应用统一标准》	×	×	√	√	×	√	√
《建筑工程设计信息模型分类和编码标准》	×	×	√	×	×	√	×
《建筑信息模型存储标准（征求意见稿）》	×	×	√	√	×	√	×
《建筑工程设计信息模型交付标准》	×	×	√		×	√	×
《建筑信息模型施工应用标准》	×	×	√	√	×	√	×

注：横坐标为 GDPR 七大原则，与表 1 对应简写；纵坐标为各项 BIM 标准文件。

3 工程信息共享安全问题及建议

3.1 工程信息安全问题总结

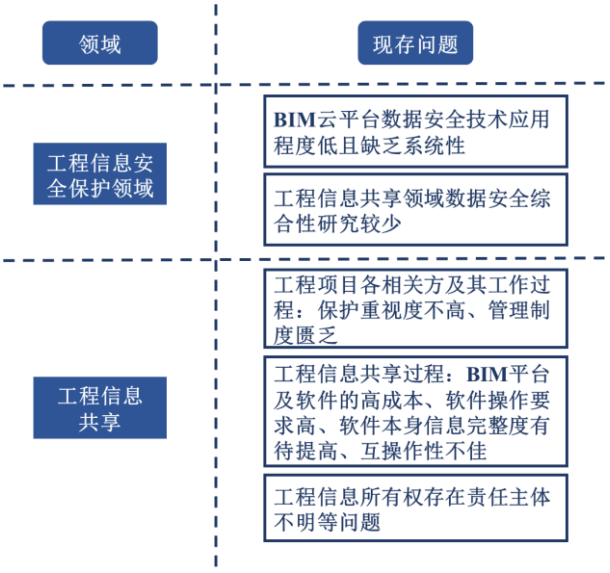

图 3 工程信息共享安全问题

通过研究当前建筑工程领域信息安全现状，本文总结归纳了如图 3 所示的现存问题：第一，BIM 云平台数据安全技术应用程度低且缺乏系统性。当前常用的 BIM 信息安全技术，如加密协议、分布式数据库系统、BIM 云、区块链技术等，虽然可将信息进行加密处理，保护工程信息传递过程中信息数据的一致性、完整性、准确性和真实性，但由于成本高、操作不便、对技术要求较高等原因，尚未得到广泛应用，同时因四种技术都存在其各自的局限性，仅使用一种信息安全保护技术难以保证 BIM 平台数据机密性及数据所有权等信息安全。第二，工程信息共享领域数据安全综合性研究较少。国内外学者关于工程信息共享的研究主要集中在信息管理效率提升和工程信息数据互用共享标准两个方面，大多数研究集中在 BIM 模型的建立和信息利用上，较为缺乏从网络安全原则、分布式环境特征、BIM 功能及建筑项目性质等角度出发对工程信息共享过程中的数据安全问题进行综合性研究。

3.2 针对安全问题的解决建议

为解决上述总结的几个问题，本文提出以下几个建议：

1、完善工程信息管理领域相关法律法规或规范标准建设。

GDPR 的数据处理原则与工程信息共享过程的机制建设具有高度适配性，因此可参考《通用数据保护条例》等数据安全领域法律法规，建立符合我国国情及行业现状的工程信息管理领域相关规定，明确工程信息所有权归属问题，明确责任各相关方的权利和义务，规范工程信息共享过程，从而达到保护工程信息传递共享过程中数据

安全的目的，为工程信息交流沟通创造良好的条件和环境，提高信息传递效率，推动建筑工程行业生产创新发展。针对表 8 所揭示的现行标准中关于数据共享机制的不足，进一步加强对于工程数据的目的限制、存储限制、问责制原则的规定。

2、加大对 BIM 技术领域的研究，进一步推广 BIM 应用。

通过完善 BIM 国家标准、加大 BIM 技术信息安全领域研究开发，提高信息安全技术应用系统性，扩大 BIM 应用范围，提高 BIM 应用标准化程度，使工程信息在项目不同阶段、不同专业人员、不同利益主体间的传递共享进一步加强，从而提高信息共享效率。

3、设立第三方机构/部门监督数据安全保护。

设立第三方数据安全监督机构，如数据保护官（Data Protection Officer）。参考《通用数据保护条例》中关于 DPO 的规定，可设立独立的网络个人信息监管机构，该机构监管各部门个人信息数据处理工作，统筹协调行使执法权限，并负责本单位企业的数据保护工作，同时，还可通过对违规企业处以高额罚款，提高处罚力度，促使机构和企业自觉加强对个人信息的保护[18]；也可参考 GDPR 以“谁管理谁负责”为原则设立数据保护官，由第三方机构或部门对工程项目过程中的信息管理、共享安全进行监督，进一步维护工程信息数据安全。

4 结语

信息化时代背景下，BIM 技术在建筑工程项目应用的不断深入，数据互用成为工程项目管理中非常重要的一环，如何保护工程信息共享过程中数据安全成为专注重点。因此，本文基于欧盟《通用数据保护条例》（GDPR）分析建筑工程信息共享机制与 GDPR 数据处理原则的适配性，并结合 GDPR 所呈现的数据处理原则研究工程信息共享过程中数据安全问题及解决方案。

随着 BIM 应用的不断深化，工程信息安全必将收到更多关注。随着技术的不断进步及法律法规的不断完善，工程信息传递将在一个更为安全的环境下进行，建筑工程的发展将在维护工程信息数据安全的同时提高信息传递效率，利用新技术集成创新，带动传统行业转型升级。

参 考 文 献

[1] 美国国家 BIM 标准第一版第一部分： National Institute of Building Sciences, United States National Building Information Modeling Standard, Version1-Part 1[R].

[2] 张建平,李丁,林佳瑞,颜钢文.BIM 在工程施工中的应用[J].施工技术,2012,41(16):10-17.

[3] Moumita Das, Xingyu Tao, Jack C.P. Cheng, BIM security: A critical review and recommendations using encryption strategy and blockchain, J. Automat. Construct. 126 (2021) 103682.

[4] V. Singh, N. Gu, X. Wang, A theoretical framework of a BIM-based multi-disciplinary collaboration platform, Autom. Constr. 20 (2) (2011) 134–144.

[5] O.A. Olatunji, A preliminary review on the legal implications of BIM and model ownership, J. Inform. Technol. Construct. 16 (2011) 687–696. Special issue Innovation in Construction e-Business, http://www.itcon.org/2011/40.

[6] K. Afsari, C. Eastman, D.R. Shelden, Cloud-based BIM data transmission: current status and challenges, in: Proceedings of the 33rd International Symposium on Automation and Robotics in Construction, Auburn, AL, USA, 2016, pp. 1073–1080.

[7] E.A. Parn, D. Edwards, Cyber threats confronting the digital built environment: common data environment vulnerabilities and blockchain deterrence, J. Eng. Construct. Architect. Manag. 26 (2) (2019) 245–266, https://doi.org/10.1108/ ECAM-03-2018-0101.

[8] Zhang, J., Liu, Q., Hu, Z., Lin, J.*, Yu, F. (2017). A Multi-Server Information-Sharing Environment for Cross-Party Collaboration on a Private Cloud. Automation in Construction, 81, 180-195. doi: 10.1016/j.autcon.2017.06.021.

[9] M.C. Badertscher, U. Maurer, A. T, P. T, Strengthening access control encryption, in: Proceedings of Advances in Cryptology – ASIACRYPT 2017 10624, 2017.

[10] M. Kassem, N. Iqbal, G. Kelly, S. Lockley, N. Dawood, Building information model: protocols for collaborative design processes, J. Inform. Technol. Construct. 19 (2014) 126–149. http://www.itcon.org/2014/7.

[11] T. Zhao, L. Wei, C. Zhang, Attribute-based encryption scheme based on SIFF, in: Proceedings of the IEEE International Conference on Communications (ICC), Kuala Lumpur, 2016, pp. 1–6, https://doi.org/10.1109/ICC.2016.7511327.

[12] N. Skandhakumar, J. Reid, F. Salim, E. Dawson, A policy model for access control using building information models, Int. J. Crit. Infrastruct. Prot. 23 (2018) 1–10, https://doi.org/10.1016/j.ijcip.2018.08.005.

[13] K. Afsari, C. Eastman, D.R. Shelden, Cloud-based BIM data transmission: current status and challenges, in: Proceedings of the 33rd International Symposium on Automation and Robotics in Construction, Auburn, AL, USA, 2016, pp. 1073–1080.
[14] J. Li, D. Greenwood, M. Kassem, Blockchain in the built environment and construction industry: a systematic review, conceptual models and practical use cases, J. Automat. Construct. 102 (2019) 288–307, https://doi.org/10.1016/j.autcon.2019.02.005.
[15] R. Zheng, J. Jiang, X. Hao, W. Ren, F. Xiong, Y. Ren, bcBIM: A Blockchain-based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud 2019, 2019, https://doi.org/10.1155/2019/5349538.
[16] 尚虎平,朱昭娜.走向基本公共服务的公民信息权保护——来自欧盟《一般数据保护条例》的启示[J].中国高校社会科学,2020(01):117-123+158-159.
[17] 王瑞.欧盟《通用数据保护条例》主要内容与影响分析[J].金融会计,2018(08):17-26.
[18] 张莉."欧盟《通用数据保护条例》对我国的启示." 保密工作 .08(2018):45-47. doi:10.19407/j.cnki.cn11-2785/d.2018.08.023.

Research on Data Security of Engineering Information Sharing Mechanism Based on GDPR Principle

DENG Hui[1], XU Yi-wen[1], LI Xiao-yao[1], DENG Yi-chuan[1], LIN Jia-rui[2]
（1. School of Civil Engineering & Transportation，South China University of Technology，Guangzhou 510641，China；
2. School of Civil Engineering, Tsinghua University, Beijing 100000, China）

Abstract： With the increasing scale and complexity of engineering projects, the application of Building Information Modeling (BIM) continues to deepen, and the Information volume stored by the engineering Information carrier represented by BIM model in each stage of the whole life cycle of construction projects gradually expands. The project information sharing not only improves the efficiency of the project construction, but also causes the practitioners to pay attention to the data security problem. The General Data Protection Regulation (GDPR) issued by the EU is the most extensive, demanding and punishing law in the field of Data security at present, setting a new international benchmark in the field of Data and information Protection. BIM model, as a single data source of engineering, has similarities with GDPR principle no matter in terms of data information scope or information security principle. Therefore, on the basis of studying the current BIM standards and specifications in China, the security requirements of software and platform and user usage protocols, this paper makes a comparative analysis of the BIM and GDPR data processing principles respectively to study their suitability. Analyse the reference significance of GDPR data processing principle to solve the problems in the field of engineering information security; Finally, some suggestions are put forward for data information security protection in the process of engineering information sharing.

Key words: Project information sharing; GDPR; Data security; BIM