463560

Sharing Data in Cloud-Based Platforms: Avoiding Risks, Liability & Disputes

May Winfield
BuroHappold

Learning Objectives

1. Learn how to prepare documents that avoid the legal and contractual risks of sharing data to external parties on cloud platforms like BIM 360
2. Learn how to implement processes that avoid the legal and contractual risks of internal data sharing on cloud platforms like BIM 360
3. Learn how to implement processes that avoid the legal and contractual risks of sharing data to external parties on cloud platforms like BIM 360
4. Learn how to improve the efficiency and reduce the legal and contractual risks of using cloud platforms like BIM 360

Description

Cloud-based platforms like BIM360 powerfully connect project teams and data. This very ability to connect however– with decisions and actions made based on the connected information – brings a host of potential misunderstandings, increased liability and risks: Who is responsible for errors/corruption in data accessed by external parties? Is the party hosting the platform responsible for misuse of the platform and data in it? What obligations do parties accessing the BIM360 or other platform have to the hosting party? It's ticking time-bomb of liability and expensive disputes waiting to happen. There are presently no resources or practical advices on how to mitigate/avoid such issues, or indeed how to explain them to your lawyers so they can help you avoid the risks. In this class, you will be given practical, useful advice on reducing risk and how to clarify parties' rights and obligations via clear process, guidance and terms.

Speaker

May is the Head of Commercial and Legal for Cities and Digital at international engineering firm, BuroHappold, where she takes the lead on legal and contractual matters relating to digital and construction technology - working closely with the business worldwide to continually improve and risk manage processes and documentation in this area. Her 16+ years as a construction lawyer and many years researching the legal and contractual aspects of construction technology has enabled her to speak the 'languages' of both legal and tech in a way each side can appreciate and implement.

Recognised as a leading legal specialist in BIM and construction technology, May provides pragmatic advice and thoughts on the legal impact of construction technology at events worldwide. May has authored and co-authored various documents in these fields, including co-authoring legal guidance on the ISO19650 BIM international standard, an ISO19650-compliant Information Protocol, and an upcoming book chapter analyzing Construction 4.0. She is co-founder and chair of BIM4Legal (a forum for lawyers and industry to increase knowledge on legal issues of BIM) and member of various other industry groups seeking to support the industry in progressing and implementing digital technology. Having first got involved in this area due to her geeky love of all things tech, many of her hobbies remain very tech-focussed – even exercise involves 'competing' on her iWatch against a number of digital directors from other consultancies.

Introduction

"I don't need a hard disk in my computer if I can get to the server faster…
carrying around these non-connected computers is byzantine by comparison"
Steve Jobs

The construction industry is undergoing a major transformation, moving steadily towards a more digital environment and Construction 4.0. We also face the related challenge of increasingly complex data and systems, and the added complexity of remote working and global data exchanges. Cloud-based platforms potentially solve many problems: reducing time; increasing agility; creating a culture of trust and sharing; and potentially even encouraging more innovative collaboration due to the easier exchange and extraction of information and data.

McKinsey 5 August 2019 Insights, 'Unlocking business acceleration in a hybrid cloud world', observed that "*The companies we surveyed [in Spring 2019] currently have around 50 percent of all workloads running on public- and private-cloud platforms. By 2022, that share is projected to rise to 75 percent, with roughly two-thirds of that workload housed in shared public platforms within data centers built out by the major cloud-service providers.*" This is likely to be much higher than predicted in the environment in which we currently find ourselves. Indeed, McKinsey pointed out on 21 July 2020 that "*Leaders need to accelerate their journey to the cloud in order to digitize quickly and effectively in the wake of COVID-19*"[1].

How are we to define cloud computing, and the resulting cloud platforms? There are various definitions but one I feel is relevant to this discussion is that cloud computing is the model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources[2]. There are three accepted categories of cloud computing services, and the issues discussed in this paper are potentially relevant to any of the three:

- *Infrastructure as a Service (IaaS):* Remote computing and storage
- *Software as a Service (SaaS):* Access to services without installation of additional software, enabling data-intensive operations being executed in the cloud
- *Platform as a Service (PaaS):* Remote access to development platforms for software without implementing the software and hardware oneself, i.e. application builders not limited by their own server power

It is now generally accepted that using cloud computing services, including cloud-based platforms like BIM360, reduces time, increases agility and facilitates a culture of trust between parties. Such platforms also encourage innovative collaboration, due to the easier extraction and recording of data and reduced fragmentation of processes and data exchanges.

As readers will be aware, the BIM 360 cloud solution seeks to aggregate data and provide transparency to project stakeholders, making everyone more accountable and improving visibility. The Autodesk Construction Cloud (https://construction.autodesk.com/vision) in turn seeks to facilitate seamlessly connected data at a time when there is a recognition that successful project

[1] McKinsey 21 July 2020 Insights: "Three actions CEOs can take to get value from cloud computing

[2] T. Mell – P. Grance, *The NIST Definition of Cloud Computing*, US Department of Commerce, 2012

delivery requires the ability to manage data on common platforms, allowing the various parties to work efficiently and easily throughout the process.

Nonetheless, such platforms are often used simply by moving legacy applications and existing systems to work on the cloud - without considering the impact on processes and the resulting new risks that need to be addressed (something McKinsey termed ‘lift-and shift’ in an Insights article in 2018). This is comparable to the prevailing mindset during the move from the drawing board to 2D CAD in the 1990s. This not only prevents parties from getting the full benefits offered by such cloud platforms but equally importantly, it lays a potential minefield of differing expectations, potential disputes and unexpected liabilities.

This industry talk seeks to consider the potential legal and contractual issues that could be caused by using cloud platforms. It provides practical suggestions to avoid and mitigate these issues and risks. It also considers ways to implement better processes to improve efficiency and effectiveness in this risk management. It is hoped this paper will provide useful, jargon-free steps to reduce risk and clarify obligations, enabling parties to work together more efficiently in the collaborative environment.

This paper is provided for general information only. It is not intended to amount to advice on which you should rely. You should obtain professional advice before taking, or refraining from taking, any action on the basis of this paper.

Preparing documents that avoid the legal and contractual risks of sharing data to external parties on cloud platforms

"*The cloud is a means, not an end*"[3]

Using a cloud-based platform is not simply a matter of moving your (and others) data from the hypothetical cardboard box of your IT systems to the new box of a remote server. There are resulting changes in processes and requirements whenever you move to something so different in form and function from what you were using prior. This in turn leads to new risks, liabilities and tasks that need to be allocated or filled. To take an example: a party provides access to its cloud storage system to its supply chain or client. There are subsequent problems with access or corruption of documents, with consequential delays or additional costs incurred. The question then becomes: who bears liability for this if the documentation is silent? Was it simply something parties had not considered and therefore not discussed? Can a party withdraw access to another party at its convenience, as occurred in the UK court case of *Trant v Mott Macdonald* [2017] EWHC 2061 (TCC) when the BIM Information Manager, Mott Macdonald, withdrew the contractor, Trant's access to the Common Data Environment due to a payment dispute. It is understood that the contract documents were silent on this issue, leading to an expensive, and time consuming, court case.

One should not underestimate the importance of setting out the roles, rights and responsibilities in the use and access of the intended cloud-based platform in binding contractual documentation. In the event there is an issue, the documentation will clarify parties' position and rights so they can then progress accordingly rather than argue back and forth over the point. From my years of experience as a construction lawyer, it is the matters on which one is silent – the gaps in the documentation – that end up being disputes, as each party's perspective will almost always be personal and different. Furthermore, one cannot only rely on the conversation one is having with the other party now; given the nature of the industry the likelihood is that a different individual will be considering this at a later date.

[3] McKinsey Insights, 'Cloud adoption to accelerate IT modernization', 12 April 2018

Ascertaining what the documents need to cover

In most cases, your legal or professional advisor is unlikely to be familiar with the functioning and processes of the cloud platform you use. They may rely on you to instruct them on the real issues and risks that need to be dealt with and clarified, so they can then incorporate this into the contractual documentation. But how do you create that list of issues and risks?

A good starting point is to take a blank piece of paper (or empty text document) and list out:

1. What are the security risks posed by using a cloud platform?
2. What are the initial processes and tasks that need to be carried out to set up the use of the cloud platform, e.g. granting access and having the correct Autodesk licences?
3. What are the main processes and tasks that need to be carried out as part of the regular exchange of data, e.g. checking data has been uploaded and named correctly and arranging back-ups of data?
4. What are the likely and/or high risk things that could go wrong, e.g. platform being unavailable for a period or your own infrastructure/bandwidth simply not being up to the task,; data becoming corrupted or third parties getting access to the data?
5. For each of the items listed in these categories, who should bear the risk or be responsible for mitigating it?
6. Does your Client have any express requirements that impact risk and arrangements, e.g. high security requirements or limitations on the location of data?

This list can then form the basis of that discussion with your professional advisor.

Supply Chain Contracts

Where access to your cloud platform is going to be given to your supply chain, from my own experience, I suggest that the below areas often prove helpful to clarify by way of both express contract clauses and discussion for sake of certainty of both parties:

1. Obligations, for example who has the obligations of arranging access to the platform and the hardware/infrastructure required to access the platform.
2. Rights, for example rights regarding maintaining or revoking access and rights regarding over the data itself.
3. Responsibilities, to put it simply is it clear who is responsible for each part of the process and for the common issues/risks or are there gaps in responsibility that need clarifying?
4. Limitations, for example the limitations on use, access and on liability for delays and costs arising from use of the platform.

Client Contracts

The nature of one’s relationship with the Client may necessitate additional express contract terms, and I’ll set out some potential main issues that should be dealt with.

Where access to the cloud platform is going to be given to your client, there may be additional issues to clarify, in particular who bears the costs of the licences – if one party bears licence costs for the other, is it clear for how long this continues? I have seen contracts over the years which appear to require a contractor or consultant to maintain licences for the Client for some years after the project is complete.

What responsibilities do you have to ensure the users access the data for particular purposes and functions? Are you responsible to the Client if someone inappropriately accesses or uses the data (and vice versa)? The *Trant v Mott Macdonald* case applies equally here, are you entitled to turn off a Client's access in the event of a fee or other dispute?

If the Client is hosting the platform, or indeed a number of platforms for different purposes (e.g. documents, models and drawings), which is the arrangement encouraged by the international standards, ISO19650, one may want to consider the previous list of queries to see how they apply to you as the party accessing the platform. Equally, is it clear how long you will have access, to ensure you have an opportunity to complete all your services or works and respond to queries or issues later on.

The Impact on Other Contract Terms

Apart from risk, roles and liability generally in the use of the platform itself, there may be other obligations and contract terms that have consequential impact on the use of a cloud platform.

Data Privacy

The GDPR in Europe (and equivalent data privacy regulations across the world) contain rigorous requirements about the handling of personal data. Autodesk's website contains comprehensive guidance (https://www.autodesk.com/trust/compliance) on their compliance with the GDPR, as well as equivalent laws in Canada and Brazil, including the recognized use of standard contract clauses to legitimize international data transfers. Does your contract require any other steps over and beyond these processes put in place for compliance with the relevant regulations?

Data Location

Check as soon as possible whether your draft contract or Client requirements have restrictions on this. It is important to bear in mind where the intended cloud servers are located, e.g. Autodesk's servers will be in Ireland or the US[4]. A contract may restrict the required location of data, e.g. to the country of the project or, for sensitive or high security installations, to the premises of the Client. In these situations, one cannot blindly use BIM360 as usual without considering this with the Client and make contract amendments to reflect the server location, as necessary. This is not a reason to panic, however. Many, or even arguably the majority, of EU-based contracts[5] provide that they accept data locations within the EU so a location in Ireland would comply. Equally, US-based contracts would usually accept data locations within the US, without a requirement for a location in a specific State for example. It is, putting it simply, necessary to check what your contract requires and ensure you comply with it or that the contract is amended to reflect what the intended location is.

[4] https://knowledge.autodesk.com/support/bim-360/learn-explore/caas/sfdcarticles/sfdcarticles/Where-are-cloud-servers-located.html

[5] and the UK, at the time of writing.

Auditing

Many contracts have express and detailed provisions about a Client’s right to carry out audits. Will the data on the cloud platform fall within the ambit of such audit and does it comply with any contractual requirements to permit the audits they have in mind? Separately, but on a related point, has there been consideration on future archiving, both archiving format and suitability, so steps can be taken early to arrange this?

Implementing processes that avoid the legal and contractual risks of internal data sharing and external data sharing on cloud platforms

The essence of cloud computing is that a customer entrusts its own digital information, together with that of third parties, to the cloud computing service provider[6]

Do People Know What They're Supposed To Be Doing?

Be aware that many people in your organisation (and those of your Client and/or project team and supply chain) may be coming at this technology or process completely new. Training is vital, but this will not be a one-size-fits-all. Some will require detailed technical training. Others, such as management and in-house legal, may require a broader overview of how the cloud platform is going to be used, the issues and risks and how these are going to be mitigated and/or recorded.

In supporting and reinforcing the training, easy-to-understand guidance notes and checklists are often handy. No one really remembers training they attended a year ago, and best practice could inadvertently fall by the wayside.

Standardisation of the use of the platform, access to the data and recording/reporting will also self-evidently manage risks and highlight when some risks are occurring or are likely to occur.

Risk Mitigation

It is essential that there are processes and records of who has – and should have - access to the platform, and what the permitted uses are. Equally, are there clear processes to restrict access and withdraw access when an employee leaves or a sub-consultant or sub-contractor is terminated? It is not unusual to hear of ex-employees or ex-project team members to continue to have access to a cloud platform for some months, as withdrawing access has simply been forgotten in the pressures of progressing the project.

[6] C. Reed, *Information "Ownership" in the Cloud*, Queen Mary University of London, Legal Studies Research Paper, 2010

Improving the efficiency and reducing the legal and contractual risks of using cloud platforms like BIM 360

Companies that adopt the cloud well bring new capabilities to market more quickly, innovate more easily, and scale more efficiently—while also reducing technology risk[7]

What Happened?

People often underestimate the importance and simple effectiveness of maintaining sufficient, reliable records. Such records are invaluable in the event of queries or disputes about the relevant work or designs during and after the project and are also internal reference and learning tools. There are also often express contractual requirements to hold information and data from a project for a certain number of years - 6 years being common. All of this necessitates back-ups being maintained but this cannot be done without forethought. If back-ups are stored within a cloud platform, which parties have (and will continue to have) access to them? Is there a need to store separate back-ups to guard against data loss? There is also no point having a long-term back-up if it cannot be accessed when needed; version control of software is a known issue that will need to be factored into the selection of the back-up format and process otherwise it could be akin to having a 3.5" floppy disc of back-up data now – you can hold it but may not be able to find anything to access any of the valuable data on it. Finally, the security of the back-ups needs to be considered, not just your own but being sufficiently comfortable with the security of the back-ups held by other members of the project team which likely contain some of your data as well. This is particularly an issue for high security or sensitive projects.

Another thing that people often underestimate is the power of simply talking to each other. Tools like cloud platforms facilitate greater collaboration, but in themselves cannot force people to collaborate. From my experience, it is often necessary or at least helpful to oblige some collaboration via binding contractual requirements, e.g. regular exchange of status updates and meetings, and frequently people will appreciate the benefits of such collaboration after being required to go through the process. When a project team is all using the same cloud platform, whether external parties or indeed an internal team, discussion and understanding of how the

[7] McKinsey 15 Sept 2020 Insights: How CIOs and CTOs can accelerate digital transformations through cloud platforms

data is being named, moved and updated. Do parties know where the latest data will be, and are they aware of when it is updated so they are working to the correct versions? Such understanding could sensibly be both in process documents, but also via the regular meetings (or online video calls for now!)

Security

Increased use and reliance of cloud platforms by its nature results in increased security risks. Some of the things to consider when deciding what reasonable steps are required to increase security include:

- Is there sufficient awareness within your organisation on how to use the cloud platform in a safe and secure way (e.g. what categories of confidential or sensitive internal documents/data should not be uploaded and shared)? Is there the same level of awareness among those parties you appoint? This may require training and encouragement of a change in mindset to take into account the new way of working on the cloud.
- What are the realistic safeguards that can and should be taken, such as limiting or avoiding downloads of the data to external storage devices?
- Who grants and monitors access to your cloud platform?
- Is there sufficiently clear and enforceable prohibitions on sharing passwords/access?

For ideas, it is worth considering the user-friendly security steps set out in the international standards, ISO19650-5, which is focussed on information management security.

Insuring Against Risk

In many ways, cloud computing is a very different way of working to what came before. It is worth considering, and discussing with your insurance broker, whether your organisation has all necessary insurances. Think of what could go wrong in using the cloud platform and ask which parts are uninsured so you can take other mitigation steps, such as excluding or limiting liability in your contract. Does your insurance cover issues arising from hosting a cloud platform or common data environment for other project team members to access?

Learning from the new international information management standards

The ISO 19650 series is the result of circa 4 years of work and collaboration of international representatives, and is, in essence, a series of standards providing best practice for information management in a digitised environment. It is therefore a very good, and up-to-date, source of best practice for information management in a cloud environment. In writing this paper, I discussed the intentions and some essential tips with the author of the ISO19650-2, Paul Shillcock, being the section of the standards for the design and construction stage of a project. I set out some key aspects below, but it is worthwhile considering the standards as a whole.

The ISO19650 envisages that the Client will set up and manage the common data environment (“CDE”)[8], including a cloud platform, for the project. There may however be a “distributed CDE” being a local environment for the delivery team to develop information and data in a work-in-progress state before sharing it onto the Client’s project CDE. Paul noted that it is important

[8] See https://constructionblog.autodesk.com/common-data-environment/ for an explanation on what a CDE is and why it matters.

parties do not simply share data to the project CDE at the end of the appointment, the point of the CDE is to facilitate collaboration and data exchange throughout the project. The manner and timings of such exchanges should usually be set out in the process documents so all parties are working consistently. At the end of a project, the ISO19650 requires a CDE Archive to be created which contains all shared and published revisions of each set of data (called ‘information containers’ by the standards) as well as an Archive Journal which holds an auditable record of who did what and when. Such archives are invaluable to establish the history of certain issues and who should bear liability. Is a Client intending to create such archives? If so, who has a right to access or view it?

Plain Language Checklist

“Cloud computing is the third wave of the digital revolution”[9]

I find checklists very useful as ways to conveniently ensure things are done and not forgotten. Below I set out a checklist summarizing the main points contained in this paper, which I hope will be useful for you in considering what processes and risk mitigation measures to implement, and terms to incorporate into your documentation to deal with the issues highlighted:

1. **Does the cloud platform and its accompanying systems comply with legal and contractual requirements?**

2. **Do the documents state who is responsible for main aspects of setup, maintenance and access?**

3. **Do the documents state who bears the likely/common risks and problems?**

4. **Do the documents clearly limit or exclude liability?**

5. **Are internal processes in place and enforced, e.g. access, use and withdrawal of access?**

6. **Are there internal records and/or back-ups?**

7. **Is there a plan for the end of the project, i.e. records and archiving**

8. **Is there sufficient/the right insurance?**

[9] Lowell McAdam, CEO of Verizon