



EAQUATQUE

Datenschutz und Datensicherheit ...

Foto: Ken Schluchtmann, diephotodesigner.de

...in der Architektur und im Ingenieurwesen – zwischen Verantwortung und Herausforderung

1. Einleitung

Die Digitalisierung verändert die Arbeitswelt in allen Branchen – auch in der Architektur und im Ingenieurwesen. Immer häufiger werden Projekte digital geplant, modelliert, verwaltet und kommuniziert. Damit steigen nicht nur die Effizienz und Präzision, sondern auch die Anforderungen an den Schutz sensibler Daten. Ob Entwurfspläne, statische Berechnungen, Energieausweise oder persönliche Daten von Bauherren: Sie alle müssen sicher gespeichert, verarbeitet und weitergegeben werden. Datenschutz und Datensicherheit sind dabei nicht nur eine technische, sondern auch eine rechtliche und ethische Verantwortung. Dieser Artikel gibt einen strukturierten Überblick über die wichtigsten Aspekte – von den Grundlagen über Risiken bis hin zu konkreten Maßnahmen und rechtlichen Pflichten beim Umgang mit Daten.

2. Datenschutz und Datensicherheit – ein Überblick

Datenschutz und Datensicherheit werden oft synonym verwendet, beschreiben aber unterschiedliche Dinge:

- **Datenschutz** betrifft den Schutz personenbezogener Daten – also aller Informationen, die sich auf eine identifizierbare Person beziehen, z. B. Namen, Adressen, Fotos oder Telefonnummern von Bauherren oder Projektbeteiligten.
- **Datensicherheit** hingegen meint den Schutz aller Daten

(auch technischer Art) vor Verlust, Manipulation oder unbefugtem Zugriff.

In der EU ist der Datenschutz durch die Datenschutz-Grundverordnung (DSGVO) geregelt. Diese schreibt unter anderem vor, dass personenbezogene Daten nur zweckgebunden, transparent und sicher verarbeitet werden dürfen. Für Architekturbüros oder Ingenieurbüros bedeutet das: Sie sind sowohl für die technische Sicherheit ihrer Systeme als auch für die rechtmäßige Verarbeitung der Daten verantwortlich – selbst dann, wenn sie externe Dienstleister einsetzen. Wer ist wofür verantwortlich?

Das Architektur- oder Ingenieurbüro ist datenschutzrechtlich der sogenannte Verantwortliche im Sinne der DSGVO. Das bedeutet:

- Es entscheidet darüber, welche personenbezogenen Daten verarbeitet werden, zu welchem Zweck und auf welche Weise.
- Es trägt die volle rechtliche Verantwortung für die Einhaltung der Datenschutzvorschriften – selbst dann, wenn die technische Umsetzung (z. B. Speicherung oder Verarbeitung) durch einen externen Dienstleister erfolgt.
- Es muss sicherstellen, dass angemessene technisch-organisatorische Maßnahmen (TOMs) zum Schutz der Daten vorhanden sind.
- Es ist verpflichtet, Verzeichnisse der Verarbeitungstätigkeiten zu führen, Betroffenenrechte umzusetzen (z. B. Auskunft, Löschung) und Datenschutzverletzungen zu melden.

Externe Dienstleister – z. B. IT-Dienstleister, Cloud-Anbieter, Softwareentwickler oder spezialisierte BIM-Plattformen – gelten in der Regel als Auftragsverarbeiter nach Art. 28 DSGVO. Das heißt:

- Sie verarbeiten personenbezogene Daten im Auftrag und nach Weisung des Architektur- oder Ingenieurbüros.
- Sie dürfen die Daten nicht für eigene Zwecke nutzen oder an Dritte weitergeben.
- Sie sind verpflichtet, die Daten angemessen zu schützen und alle Vorgaben des Verantwortlichen umzusetzen.

Wichtig: Für jede Zusammenarbeit mit einem externen Dienstleister, der Zugriff auf personenbezogene Daten hat, sollte ein schriftlicher Auftragsverarbeitungsvertrag (AVV) abgeschlossen werden. Dieser regelt,

- welche Daten verarbeitet werden dürfen,
- wie lange sie gespeichert werden,
- welche Sicherheitsmaßnahmen gelten,
- und welche Rechte und Pflichten beide Seiten haben.

Fehlt ein solcher Vertrag, oder verstößt der Dienstleister gegen Datenschutzvorgaben, haftet in erster Linie das Büro – nicht der Dienstleister. Das bedeutet ein erhebliches Risiko für Bußgelder, Reputationsschäden und rechtliche Auseinandersetzungen.

Ein kurzes Beispiel hierzu:

Ein Architekturbüro nutzt eine externe BIM-Cloud-Plattform zur Koordination der Planung mit verschiedenen Fachplanern. Die Plattform hostet auch personenbezogene Daten (z. B. Name, Anschrift des Bauherrn). Das Büro ist verantwortlich für die Auswahl einer datenschutzkonformen Lösung, für die vertragliche Absicherung und die Einhaltung der Zugriffskontrollen – nicht der Plattformbetreiber allein.

3. Risiken für Architekten und Ingenieure

Der Umgang mit Daten in der Planung und Ausführung von Bauprojekten birgt konkrete Risiken. Hierzu zählen unter anderem:

- Cyberangriffe auf Server oder Cloud-Systeme, bei denen Pläne oder Berechnungen gestohlen oder verändert werden können.



Foto: Ken Schluchtmann, diephotodesigner.de

- Verlust von Daten durch Systemfehler oder menschliches Versagen, etwa bei nicht gesicherten Backups.
- Datenpannen durch unverschlüsselte Kommunikation oder ungeschützte Endgeräte auf der Baustelle.

Diese Vorfälle sind nicht nur teuer und imageschädigend – sie können auch haftungsrechtliche Konsequenzen nach sich ziehen, etwa bei der Weitergabe personenbezogener Daten ohne Einwilligung oder bei mangelhaften technischen Schutzmaßnahmen.

4. Building Information Modeling (BIM) – Fortschritt mit Schattenseite?

Ein zentrales Werkzeug der Digitalisierung im Bauwesen ist das Building Information Modeling (BIM) – die modellbasierte, digitale Planung, Ausführung und Bewirtschaftung von Bauwerken. Dabei werden sämtliche relevanten Informatio-



Foto: Ken Schluchtmann, diephotodesigner.de



Foto: Ken Schluchtmann, diephotodesigner.de

nen in einem zentralen Datenmodell zusammengeführt und allen Beteiligten zugänglich gemacht.

Doch je mehr Daten zentral verarbeitet und geteilt werden, desto größer ist das Risiko von Datenmissbrauch oder -verlust. Fragen wie „Wer darf auf welche Daten zugreifen?“, „Wie werden diese Daten geschützt?“ oder „Wie werden Zugriffsrechte geregelt?“ sind essenziell. Besonders kritisch ist der Umgang mit personenbezogenen Daten in BIM-Projekten, etwa bei der Planung von Wohnungen oder bei der Integration von Nutzerprofilen in Smart-Building-Konzepten. Die rechtssichere Anwendung von BIM setzt daher nicht nur technisches Wissen voraus, sondern auch ein bewusstes Datenmanagement und vertragliche Regelungen, z. B. in BIM-Abwicklungsplänen (BAP), die Rollen, Verantwortlichkeiten und Datenschutzvorgaben festlegen.

5. Best Practices und Schutzmaßnahmen

Datenschutz und Datensicherheit beginnen im Alltag – und müssen systematisch geplant und umgesetzt werden. Hier sind zentrale Maßnahmen, die jedes Architekturbüro und Ingenieurbüro beachten sollte:

- Technisch-organisatorische Maßnahmen (TOMs): z. B. Firewall, Virenschutz, regelmäßige Backups, verschlüsselte Datenspeicherung und -übertragung.
- Zugriffsmanagement: Klare Vergabe von Nutzerrollen und -rechten, z. B. über ein Rollen- und Berechtigungskonzept.
- Schulungen für Mitarbeitende: Datenschutz lebt vom Verständnis und der Mitwirkung aller – regelmäßige Schulungen sind Pflicht.
- Verzeichnis der Verarbeitungstätigkeiten: Dokumentation aller Datenverarbeitungen nach Art. 30 DSGVO.
- Privacy by Design & Default: Schon bei der Planung von IT-Systemen oder Projekten sollte der Datenschutz mitgedacht werden – z. B. durch Minimierung der Datenerhebung und datensparsame Voreinstellungen.



Autor



Peter Bertram

Produktmanagement & Underwriting Cyber
HDI Versicherung AG

Fazit



Datenschutz und Datensicherheit sind für Architekten und Ingenieure weit mehr als ein bürokratischer Mehraufwand – sie sind ein integraler Bestandteil professioneller, verantwortungsvoller und zukunftsfähiger Projektarbeit. Gerade in Zeiten von BIM, Smart Building und Cloud-Lösungen entscheidet der bewusste Umgang mit Daten über den Erfolg von Projekten – rechtlich, technisch und wirtschaftlich.

Ein solides Datenschutzkonzept schützt nicht nur sensible Informationen, sondern auch das Vertrauen der Auftraggeber, die Qualität der Arbeit und letztlich die eigene Existenz. Es ist daher höchste Zeit, Datenschutz nicht nur als Pflicht, sondern als Chance zu begreifen: für mehr Transparenz, Sicherheit und digitale Souveränität im Planungsalltag.

Auch bei bestmöglicher technischer und organisatorischer Vorsorge bleibt ein Restrisiko bestehen – denn absolute Sicherheit gibt es nicht. Genau hier setzt der Abschluss einer Cyberversicherung an. Sie ermöglicht einen gezielten Risikotransfer, wenn es trotz aller Vorsichtsmaßnahmen zu einem IT-Sicherheitsvorfall, Datenverlust oder Datenschutzverstoß kommt.

Die Cyberversicherung deckt dabei nicht nur den finanziellen Schaden ab, sondern bietet auch aktive Unterstützungsleistungen im Krisenfall. Dazu zählen etwa:

- IT-Forensik und Datenwiederherstellung nach einem Angriff,
- Kostenübernahme bei Betriebsunterbrechungen durch Systemausfälle,
- rechtliche Beratung bei DSGVO-Verstößen oder behördlichen Prüfungen,
- sowie Hilfe im Umgang mit Imageschäden, z. B. durch PR-Beratung.

Die HDI Cyberversicherung bietet neben dem Versicherungsschutz auch kostenneutrale Präventionsbausteine, die helfen können, das Sicherheitsniveau zu erhöhen:

- Der HDI Datenschutz Quick-Check analysiert, wie gut datenschutzrechtliche Anforderungen im Büro bereits umgesetzt sind – und zeigt konkreten Verbesserungsbedarf auf.
- Über das Mitarbeitenden-Präventionsangebot von Perseus erhalten Architekturbüros Zugang zu praxisnahen Awareness-Schulungen, die das Sicherheitsbewusstsein im Team stärken und Alltagsrisiken minimieren helfen.

Gerade für kleine und mittlere Büros ist eine Cyberversicherung damit eine sinnvolle Ergänzung zu internen Schutzmaßnahmen – und ein entscheidender Baustein für digitale Sicherheit und unternehmerische Stabilität im Projektgeschäft.