FAGES
Schweizerischer Fachverband Gebäudeschadstoffe
Association Professionelle des Polluants du Bâtiment

Entwurf vom 18.08.2024 zur Vernehmlassung

Privacy Code of Conduct

für begutachtende und baubegleitende Tätigkeiten im Bereich Gebäudeschadstoffe

Präambel

Die Mitglieder der FAGES führen als Mitarbeitende eines Unternehmens oder in Ausübung eines freien Berufes eine begutachtende und baubegleitende Tätigkeit aus. Diese bezieht sich auf Schadstoffbelastungen in Gebäuden (Gebäudeschadstoffe), deren Ursache, Sanierung und Entsorgung sowie Gefährdung der Umwelt, der Gesundheit oder des Wohlbefindens von Personen. Die Arbeiten erfordern einen hohen Sachverstand und seitens des Auftraggebers viel Vertrauen in die Dienstleister. Erreicht wird das mit einer möglichst wahren und nachvollziehbaren Darstellung der Sachlage, die nichts Relevantes unterschlägt, sowie mit einem Vorgehen und einer Beurteilung der Sachlage nach anerkannten Regeln. Die entsprechende Dokumentation ist unerlässlich, respektive von den Standesregeln oder von Behörden gefordert, kann u.U. aber Persönlichkeitsrechte betreffen.

Die Einhaltung des Datenschutzes erfolgt risikobasiert und verhältnismässig. Datenverantwortliche und -bearbeitende haben, für die in ihrer Verantwortung bearbeiteten Personendaten, ein angemessenes Schutzniveau festzulegen und umzusetzen. Bei einer solchen Entscheidung müssen sie Faktoren wie den Stand der Technik, die Implementierungskosten, die Art, den Umfang, den Kontext und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für betroffene Personen berücksichtigen. Infolgedessen sind sie dafür verantwortlich, das erforderliche Schutzniveau für die von ihnen bearbeiteten Personendaten selbst zu bestimmen. Der Verhaltenskodex des FAGES, welcher auf einer Datenschutz-Folgeabschätzung basiert, bietet für dessen Anwender in diesem Szenario eine wertvolle Hilfestellung. Dank einer Beurteilung durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bietet der Kodex eine gewisse, jedoch nicht absolute Rechtssicherheit.

Verpflichtung

Unternehmen und Freiberufler, welche sich freiwillig diesem pCoC unterstellen, nachfolgend als «**wir**»/«**uns**» bezeichnet, verpflichten sich im Zusammenhang mit ihrer untersuchenden oder baubegleitenden Tätigkeit im Bereich Gebäudeschadstoffe, bei der Bearbeitungen von Personendaten und auch besonders schützenswerten Sachdaten, die hier festgelegten Regeln umzusetzen.

Unsere oberste Leitung in der Schweiz bekennt sich zum Schweizer Datenschutz und dem. FAGES – Privacy Code of Conduct.

Unterzeichnet:

I. Allgemeines zum FAGES Privacy Code of Conduct

Rechtliches

Rechtliche Grundlage dieses Verhaltenskodex (Code of Conduct)

Dieser auf den Datenschutz bezogene Verhaltenskodex (Privacy Code of Conduct, pCoC) basiert auf Schweizer Recht, insbesondere dem Datenschutzgesetz (DSG, Stand 1.9.2023).

Nutzungsrecht und Anwendungspflicht

Der Schweizer Fachverband Gebäudeschadstoffe (FAGES) ist ein Berufsverband, dem Berufsleute und nicht Unternehmen angehören. Deshalb kann der Verband seinen pCoC für Unternehmen nicht als verbindlich erklären.

Unternehmen welche Schadstoffe in Gebäuden begutachten und/oder Fachplanungen/-Bauleitungen bei Sanierungen von Gebäudeschadstoffen übernehmen, und in denen FAGES-Mitglieder als Bauschadstoff-Dignostiker:in oder RLQ-Fachperson mitarbeiten, können sich freiwillig zu diesen Verhaltensregeln bekennen, ebenso freiberufliche Fachpersonen. Dies machen sie der FAGES gegenüber und nach aussen bekannt.

Gegenstand und Anwendungsbereich

Gegenstand dieses Verhaltenskodex

Der pCoC hat den Anspruch, mit dem festgelegte Verhalten, die Einhaltung des Datenschutzes bei der Bearbeitung von Personendaten für folgenden Tätigkeiten sicherzustellen:

- Bauschadstoffdiagnostik i.S.v. BauAV, VVEA Modul Bauabfälle (Tätigkeit: begutachten)
- Innenraumdiagnostik durch RLQ-Fachpersonen (Tätigkeit: begutachten)
- Fachplanung und -bauleitung bei Gebäudeschadstoff-Sanierungen (Tätigkeit: begleiten)
- Fachberatung zu Gebäudeschadstoffen bei Um- und Neubauprojekten

Anwendungsbereich und Abgrenzung

Dieser pCoC beschränkt sich auf die Erfüllung eines Werkvertrages oder Auftrages für eine Begutachtung oder Baubegleitung durch unseren Bereich Gebäudeschadstoffe.

Viele Datenschutz-Massnahmen werden im Betrieb typischerweise übergeordnet, einheitlich geregelt. Auch dann haben sie diesem pCoC zu entsprechen.

Die Datenbearbeitungen «nur» als Auftragsverarbeiter i.S.v. Art. 9 DSG oder auch ausserhalb der eigentlichen begutachtenden oder baubegleitenden Tätigkeit (z.B. für andere Leistungserbringungen des Betriebs, für das Personal- und Rechnungswesen, das Marketing, den Betrieb von Web-Sites, für allgemeine Bearbeitung von Emails und Kontaktdaten, für Forschung und Entwicklung etc.) sind nicht Gegenstand dieses pCoC.

FAGES - Good Practice Privacy

Die FAGES - Good Practice Privacy stellt eine Praxishilfe zur Umsetzung dieses pCoC dar. Sie erspart dem Anwender, die in dieser Hilfe beschriebenen Bearbeitungen von Personendaten, selber mit pCoC konformen Prozessen zu validieren. Für die beschriebene Datenbearbeitung ist, wo angezeigt, im Anhang eine Datenschutz-Folgeabschätzung vorhanden. Des Weiteren in dessen Anhang, ein Glossar zu Abkürzungen und Begriffen.

II. Betriebliche Voraussetzungen

Wir sind ein dem Schweizer Recht und dem Datenschutzgesetz des Bundes unterstellter Dienstleistungsbetrieb, welcher evtl. nebst andern, die diesem pCoC unterstellten Leistungen im Bereich Gebäudeschadstoffe erbringt.

Zu unseren Kunden gehören natürliche Personen, juristische Privatpersonen sowie Organe des öffentlichen Rechts (O.d.ö.R.), Unsere Kunden des Bereichs Gebäudeschadstoffe sind i.d.R. in der Schweiz domiziliert, können aber auch aus der ganzen Welt kommen, dann aber meist mit einer Vertretung in der Schweiz. Die Objekte, die wir untersuchen oder deren Sanierung wir begleiten, befinden sich grundsätzlich in der Schweiz.

Verantwortung des Managements

Wir als Geschäftsführung unseres Betriebes in der Schweiz, sind verantwortlich für unsere Bearbeitung von Personendaten sowie die dabei evtl. unabsichtlichen oder gar in Kauf genommene Persönlichkeitsverletzung.

Wir sind auch verantwortlich für die Bearbeitung von Personendaten durch Dritte, wenn diese die Personendaten als Auftragsbearbeiter bearbeiten. Eine solche, umfangreiche Bearbeitung vergeben wir mit einem Auftragsbearbeitungsvertrag, welcher die Bearbeitung von Personendaten im Einklang mit den Anforderungen des pCoC festlegt.

Unser Management steht in der gesetzlichen Pflicht, technische und organisatorische Massnahmen zu ergreifen, um eine unnötige Persönlichkeitsverletzung zu vermeiden und ungerechtfertigte auszuschliessen. Der Verantwortliche:

- identifiziert Bearbeitungen von Personendaten im Betrieb sowie mögliche Datenschutzverletzungen und hohe Risiken für natürliche Personen
- definiert und überwacht technische und organisatorische Massnahmen
- stellt eine angemessene Transparenz bez. der Bearbeitung von Personendaten sicher
- gewährleistet den Datenschutz bei Vertragsabschlüssen, insbesondere bei Auftragsbearbeitungen und bei einer Möglichkeit einer Bekanntgabe von Personendaten in einen Staat mit keinem ausreichenden Datenschutz
- nimmt die Rechte betroffener Personen bezüglich der Bearbeitung ihrer Personendaten im Sinne des DSG wahr oder, falls erforderlich, die Rechte betroffener Personen aus dem EWR im Sinne der DSGVO
- bestimmt eine Anlaufstelle für Betroffene, welche auch als Meldestelle für vermutete oder tatsächliche Datenschutzverletzungen dient und in diesem Fall adäquate Massnahmen ergreift (Information von EDÖB und Betroffenen bei einer Datenpanne etc.)
- sorgt für eine Unterweisung und Sensibilisierung unserer Mitarbeitenden und Auftragsbearbeiter bezüglich unserem Datenschutz und fördert im Betrieb eine datenschutzfreundliche Kultur.

Infrastruktur für den Bereich Gebäudeschadstoffe

Unser Betrieb stellt unserem Bereich Gebäudeschadstoffe, die für dessen Aufgaben erforderliche, zweckmässige und angemessen sichere Infrastruktur zur Verfügung. Sie ist an unsere Betriebsgrösse und das damit verbundenen Risiko sowie an unsere finanziellen Möglichkeiten angepasst, dies jedoch nicht unter Inkaufnahme eines nicht akzeptablen Risikos für eine Persönlichkeitsverletzung.

Räume

Wir bearbeiten Personendaten in unterschiedlich geschützten Räumen. Dabei unterscheiden wir:

- standardmässig geschützte eigene Räume, mindestens mit Sicherheitsschloss abschliessbar und ohne Anwesenheit unbeobachteter, betriebsfremder Personen
- eigene Räume mit hohem Schutz, welche zusätzlich über eine Brand- und Einbruch-Meldeanlage verfügen
- Räume ohne ausreichenden Schutz.

Eine Bürogemeinschaft oder Home-Office beurteilen wir diesbezüglich im Einzelfall und berücksichtigen dabei adäquat deren Rahmenbedingungen.

Netzwerkinfrastruktur

Zum Datentransfer und zur zentralen Datenhaltung verwenden wir Netzwerkgeräte, Netzwerke und Dienste, welche alle durch unseren IT-Berater als «sicher» eingestuft sind. Sicherheitsupdates der Hersteller für Firmware, Operating-Systems und Apps von Netzwerkgeräten werden zeitnah installiert.

- Wir verwenden eigene Daten-Server und Backup-Server (das kann auch ein Server in CH/EWR sein, auch ein virtueller, welcher ein Auftragsbearbeiter für uns betreibt), evt. auch einen dezentralen Abteilungs-Server. Mit individualisierten Zugriffsrechten und einem adäquaten Zugriffsschutz, Schutz vor Datenverlust oder -veränderung sowie einer angemessenen Ausfallsicherheit gewährleisten unsere Server eine **hohe Sicherheit**. Bei deren Auslegung berücksichtigen wir auch die Sicherheit ihres Standortes.
- Eine **hohe Sicherheit** für die interne Datenübertragung bieten Direktverbindungen über USB, als auch unser eigenes lokales Netzwerk (LAN oder gesichertes WLAN), welches mit einer Firewall gegenüber dem Internet gesichert ist. Eigene über VPN zusammengeschlossene LAN an verschiedenen Standorten oder die Anbindung eines eigenen externen Servers über VPN, gelten als ein und dasselbe LAN.
- LAN oder gesicherte WLAN von Gastnetzwerken betrachten wir i.d.R. als **sicher**, sie sind einer mit SSL/TLS geschützten Internetverbindung gleichgestellt. Den unsicheren Internetzugang über ein öffentliches WLAN oder eine Internetverbindung ohne SSL/TLS nutzen wir nicht zur Übertragung von Personendaten.

Netzwerkdienste

Unter der Bedingung eines sicheren Übertragungswegs, nutzen wir folgende Dienste zur angemessen **sicheren** Kommunikation:

- Protokolle SMTP und POP für das Versenden und Empfangen von Emails
- HTTPS für einen Web-Site Zugriff und Downloads von Dateien
- SFTP zum Transferieren von Dateien, dabei muss jedoch auch das Datenschutzniveau des Landes und der Zugriffsschutz am Speicherort der Datei ausreichend sicher sein (mindestens eine Single Faktor Authentifizierung)
- Messenger-, Meeting- und Kollaborations-Diensten, bei denen keine Daten in ein Land mit einem ungenügenden Datenschutz gelangen, ausser Standardvertragsklauseln gewährleisten einen vergleichbaren Schutz.

Wenn für die Übertragung eine **hohe Sicherheit** gefordert ist, muss über das Internet der schützenswerte Inhalt End to End verschlüsselt übertragen werden (mind. 256 Bit).

Alternativ stehen weitere Übermittlungen mit hoher Sicherheit zur Verfügung:

- Short Message Service (SMS), z.B. zur Weitergabe von Passwörtern
- ein Telefongespräch oder eine persönliche Begegnung unter Ausschluss unberechtigter Dritter
- Daten in Papierform mit eingeschriebenem Brief oder Paket, immer persönlich an eine berechtigte, natürliche Person adressiert.

Generell nutzen wir zum Übertragen von Personendaten keine Telefaxe oder kostenlose Cloud-Dienste.

Arbeitsgeräte und Peripheriegeräte

Zum Bearbeiten von Sach- und Personendaten im Rahmen ihrer Mitarbeit, stellen wir unseren Mitarbeitenden zweckmässige Arbeitsgeräte mit den erforderlichen Apps, inkl. erforderliche oder gewünschte Peripheriegeräte zur Verfügung. Alle Geräte und installierten Apps werden vor ihrer Freigabe durch eine IT-Fachperson auf ihre Zweckmässigkeit und Sicherheit geprüft. Nicht freigegebene Geräte und Apps sind im Betrieb nicht erlaubt. Wir unterscheiden dabei aus der Sicht der Datensicherheit folgende Geräte-Kategorien:

- **bedingt sicher:** Geräte zur Datenerfassung, wie Bildaufnahmegeräte, Diktiergeräte und Messgeräte ohne verschlüsselten Datenspeicher oder ohne Zugangsschutz
- **sicher:** mobile oder stationäre Arbeitsstationen, auf welche nur Mitarbeitende Zugriff haben, die Geräte befinden sich ausschliesslich in einem ausreichend geschützte Betriebsraum oder ihr Datenspeicher ist verschlüsselt (AES-256 oder gleichwertig)
- **hohe Sicherheit**: sichere Arbeitsstationen, auf deren Datenspeicher mit Personendaten nur eine zur Bearbeitung dieser Daten berechtigte Person zugreifen kann und deren sensible Daten zeitnah gesichert werden
- **Peripheriegeräte:** PC-Eingabegeräte (Tastatur, Maus), Scanner, Drucker etc.

Die sicheren Geräte werden unsererseits mit den entsprechenden Sicherheits-Updates der Hersteller aktuell gehalten und werden nur mit aktueller Software zur Abwehr von Malware betrieben.

III. Begutachtende & baubegleitende Tätigkeit

Allgemeine Beschreibung unserer Tätigkeit und deren Zweck

Unser Bereich Gebäudeschadstoffe führt die im **Kapitel I** als «Gegenstand dieses Kodex» genannten Tätigkeiten oder auch nur einen Teil dieser aus. Diese beziehen sich auf ganzen Gebäude oder auch nur einzelne Räume, was wir nachfolgend als **Objekte** bezeichnen. Dabei werden vor allem Sachdaten, i.d.R. nur wenige mit einem Personenbezug bearbeitet. Wenn der Auftrag Privatbereiche oder Beschwerden von Raumnutzenden zum Gegenstand hat, entstehen daraus u.U. auch besonders schützenswerte Personendaten.

Wir bearbeiten Personendaten zum Schutz von Mensch und Umwelt, z.T. auch zum Besitzstandschutz. Dies geschieht aus einem privaten Interesse von Betroffenen oder im Interesse der Öffentlichkeit (Vermeidung einer Umweltgefährdung).

Weiter bearbeiten wir auch Personendaten, um unserer Nachweispflicht und den Anforderungen an die Dokumentation der festgestellten Tatsachen zu entsprechen.

Unsere grundlegenden Prinzipien im Umgang mit Personendaten

Für unseren Tätigkeitsbereich Gebäudeschadstoffe gelten die nachfolgenden grundlegenden Prinzipien und Massnahmen. Grundsätzlich bearbeiten wir Personendaten ohne Einwilligung der Betroffenen. **Stattdessen ergreifen wir folgende Massnahmen:**

M01 Personendaten werden bei uns nur durch Mitarbeitende bearbeitet, welche dazu berechtigt, sowie mit unserer Datenstruktur und unseren Datenschutzregeln vertraut sind und die zu besonders sorgsamem Umgang mit Personendaten und zur Wahrung vertraulicher Informationen ausserhalb unseres Betriebes, während und nach Beendigung des Arbeitsverhältnisses, verpflichtet sind.

M02 Wir vereinbaren mit unseren Auftragsbearbeitern und Auftraggebern, wenn deren Vertretung von uns Personendaten erhält, auch mit ihr:

a) Daten mit einem Personenbezug gemäss dem Schweizer Datenschutz zu bearbeiten und dies ausschliesslich zum bestimmungsgemässen Zweck

b) die erhaltenen Personendaten grundsätzlich nur in Staaten mit angemessenem Datenschutz bekannt zu machen, in Ländern mit unzureichendem Datenschutz die Bekanntgabe von vorhandenen Standarddatenschutzklauseln abhängig zu machen

c) unsererseits die Daten gemäss dem FAGES Privacy Code of Conduct zu bearbeiten.

M03 Wir wenden ein adäquates Schutzniveau an:

a) ausschliessliche Verwendung von bezüglich ihrer Aufgabe als zweckmässig und sicher validierten Netzen, Geräten, Apps und Diensten

b) grundsätzliche Anwendung unseres Standard-Sicherheitsniveaus

c) Anwendung eines Niveaus mit hoher Sicherheit für besonders schützenswerte Daten

d) Verschiebung von Personendaten, vor allem von besonders schützenswerten, in einen Speicher mit höherem Schutzniveau, wenn es die Situation erlaubt

e) Sicherung von zentral gehaltenen, aktiven sowie archivierten Arbeitsdaten als Backup; Wiederherstellung von Backups[#R] nur gerechtfertigt und protokolliert.

M04 Wir lenken die Daten gemäss folgenden Grundsätzen (Datenmanagement):

a) Verwendung einer übersichtlichen Datenstruktur, in der sich Berechtigungen gruppieren und einfach verwalten lassen

b) Bearbeitung grundsätzlich nur von erforderlichen Personendaten und Löschung von nicht mehr erforderlichen Personendaten (dies gilt spätestens ein Jahr nach Ablauf der Verjährung auch für archivierte Dossiers)

c) Speicherung in ein objektbezogenes, zentrales Arbeits-Dossier[#R] mit einem hohen Schutzniveau und einer restriktiven Gewährung von Rechten, mit der Möglichkeit der Spiegelung auf «Arbeitsstationen mit hohem Sicherheitsniveau» von Berechtigten (das lokale und das zentrale Verzeichnis sind in diesem Falle über einen Übertragungsweg mit hoher Sicherheit zu synchronisieren)

d) zeitnahe Archivierung der Arbeitsdossiers[#R] nach Auftragsabschluss, damit die Berechtigungen weiter eingeschränkt werden und insbesondere der Inhalt nicht mehr verändert werden kann

e) Reaktivierung von archivierten Dossiers[#R] ausschliesslich gerechtfertigt und protokolliert mit Nennung des Grundes.

M05 Wir informieren betroffene Personen über die Bearbeitung ihrer Daten transparent und zeigen ihnen ihre Rechte auf:

a) generell auf unserer Homepage

b) spezifisch im Voraus einer Tätigkeit für die eine Information angezeigt ist, mit konkreter Aufforderung Betroffener, zur Vermeidung unerwünschter Datenerhebungen mitzuwirken (z.B. Entfernung/Verhüllung von nicht auf Fotos Abzubildendem)

c) auf ihren Antrag auf Auskunft zur eigenen Person.

M06 Wir bearbeiten Daten aus Begehungen und Probenahmen von Untersuchungsobjekten verhältnismässig und verantwortungsvoll, insbesondere:

a) Notizen zu Feststellungen, selten welche mit einem Personenbezug

b) Bildaufnahmen aus dem Privatbereich[#R] und Daten zu Proben**,** grundsätzlich zu einem nicht personenbezogenen Zweck i.S.v. Art. 31. Abs. 2 lit. e DSG, über Abweichungen informieren wir die Betroffenen unter Nennung des Grundes.

M07 Wir dokumentieren Mess- und Analyseergebnisse sowie daraus berechnete weitere physikalische und chemische Parameter und graphische Darstellungen davon:

a) objektiv, verzichten dabei auf ein automatisiertes Zusammenführen von Daten aus verschiedenen Quellen[#R], auf Verwendung von Algorithmen oder neuen Technologien[#R] welche maschinell einen Personenbezug herzustellen und auf die Weitergabe von Daten an Dritte, welche mit diesen solche Methoden anwenden könnten

b) bei personenbezogenen Ergebnissen (Exposition, Dosis) pseudonymisiert.

M08 Wir machen Unterauftragnehmern, Personen mit denen wir Fachwissen teilen oder Forschenden, Daten grundsätzlich anonymisiert oder pseudonymisiert bekannt.

M09 Wir erstellen unsere begutachtenden Berichte mit besonders schützenswerten Daten so, dass:

a) die enthaltene Schlussfolgerung verhältnismässig formuliert ist und eine natürliche Person (i.d.R. ohne namentliche Nennung) nur erheblich belastet, wenn ein Gesetz oder eine im Auftrag enthaltene Fragestellung dies rechtfertigen

b) ein unübersehbarer Hinweis Dritte auffordert, die genannte Zweckbindung der Personendaten ebenfalls einzuhalten.

M10 Wir führen für Bearbeitungen mit dem Potenzial eines hohen Risikos für Betroffene, vorgängig eine Datenschutz-Folgeabschätzung durch und senken ein verbliebenes Risiko mit weiteren technischen und organisatorischen Massnahmen auf ein vertretbares Niveau.

Hingegen machen wir nur mit ausdrücklicher Einwilligung der betroffenen Person oder deren gesetzlichen Vertretung i.S.v. Art. 6 Abs. 6 DSG:

a) besonders schützenswerte Personendaten[#R] ausserhalb der bestellten, begutachtenden Berichte Dritten bekannt

b) Ton- oder Bildaufnahmen von erkennbaren natürlichen Personen

c) Abweichungen von M01 bis M09 zu Lasten der Person.

#R Evtl., ohne adäquate Massnahmen, Daten mit einem Potenzial eines hohen Risikos für Betroffene