Datenschutz in Ingenieurbüros

Anforderungen durch die europäische Datenschutz-Grundverordnung

von **Ralf Wickert**

Am 25. Mai tritt die europäische Datenschutz-Grundverordnung in Kraft. Das bisherige nationale Datenschutzrecht und hier insbesondere das auf Ingenieurbüros anwendbare Bundesdatenschutzgesetz tritt außer Kraft und wird durch ein neues Bundesdatenschutzgesetz ersetzt, das allerdings seinen Rechtscharakter vollkommen ändert, weil es nur noch in den Bereichen Regelungen trifft, wo dies durch die Datenschutz-Grundverordnung zugelassen ist.

Was regelt der Datenschutz?

Ab 25. Mai gelten dann für Ingenieurbüros sowohl die EU-Datenschutz-Grundverordnung (EU-DSGVO) als auch das neue Bundesdatenschutzgesetz, das ebenfalls am 25. Mai in Kraft tritt.

Beim Datenschutz geht es – wie das Wort schon sagt – um den Schutz personenbezogener Daten natürlicher Personen. Dies können neben den klassischen Daten wie Name und Anschrift sowie Mailadresse und Telefonnummer auch Bankdaten sowie Daten zur beruflichen Tätigkeit und private Vorlieben sein. Personenbezogene Daten im Sinne des Datenschutzrechts sind also alle Merkmale, die auf eine natürliche Person hindeuten. Da der Begriff der personenbezogenen Daten sehr weit gefasst ist, finden sich auch in der Arbeit von Ingenieuren sehr viele personenbezogene Daten, z. B. Bauherren- und Grundstückdaten, Baugenehmigungsanträge, Ausschreibungen für Bauvorhaben natürlicher Personen sowie etwa Kostenschätzungen für solche Bauvorhaben.

Daneben genießen auch die Arbeitnehmer, die in Ingenieurbüros tätig sind, den Schutz der EU-DSGVO. Daher sollten sich alle Büroinhaber mit datenschutzrechtlichen Fragen auseinandersetzen und Maßnahmen treffen, um den Datenschutz dem Gesetz entsprechend zu regeln.

Die erste Frage, die sich üblicherweise stellt, ist die Frage, ob in einem Ingenieurbüro ein betrieblicher Datenschutzbeauftragter zu bestellen ist. Hier hat die Bundesrepublik Deutschland im § 38 BDSG neu von einer Regelungsmöglichkeit Gebrauch gemacht, die Art. 37 Abs. 4 Datenschutz-Grundverordnung eröffnet. Danach gilt auch nach dem 25. Mai 2018 das bisher gültige Prinzip, wonach ein betrieblicher Datenschutzbeauftragter zu bestellen ist, wenn mindestens zehn Personen regelmäßig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Hat also das Ingenieurbüro zehn Mitarbeiter, greift die Bestellpflicht für einen betrieblichen Datenschutzbeauftragten. Dies jedenfalls dann, wenn diese Mitarbeiter regelmäßig bei der EDV-mäßigen Bearbeitung von Bauvorhaben auch den Namen des Bauherren speichern.

Interner oder externer Datenschutzbeauftragter?

Sodann stellt sich die Frage, ob ein sogenannter interner betrieblicher Datenschutzbeauftragter oder ein externer betrieblicher Datenschutzbeauftragter bestellt wird. Letzterer ist Dienstleister und erledigt den Datenschutz aufgrund eines entsprechenden Dienstleistungsvertrages, während der erstgenannte in aller Regel Arbeitnehmer des Ingenieurbüros ist. Wird ein interner Datenschutzbeauftragter bestellt, genießt dieser besonderen Kündigungsschutz und kann als Arbeitnehmer praktisch nur noch aus wichtigem Grund gekündigt werden. Damit will der Gesetzgeber absichern, dass auch wirklich eine weisungsfreie Umsetzung des Datenschutzes gelingt und der Inhaber des Ingenieurbüros nicht über seine Arbeitgeberstellung entsprechenden Druck aufbaut. Weiterhin sollte sich der Büroinhaber klar sein, dass ein interner Datenschützer ausgebildet werden muss und eine entsprechende zeitliche Freiheit braucht, seinen gesetzlichen Aufgaben nachzukommen.

Welche Anforderungen stellt die EU-DSGVO noch?

Ist die Frage der Bestellpflicht eines Datenschutzbeauftragten für das Ingenieurbüro geklärt, geht es um die weitere Umsetzung der Anforderungen der Datenschutz-Grundverordnung. Hier muss zunächst erfasst werden, welche routinemäßigen Verarbeitungsprozesse in einem Ingenieurbüro auftreten. Betrachtet man den klassischen Workflow in einem Ingenieurbüro, so dürfte etwa die Anfrage eines privaten Bauherrn, für diesen tätig zu werden, das Anlegen einer Kundenakte und eines Kundenstammblattes mit sich bringen, so dass bestimmte Daten des Bauherr im System des Ingenieurbüros abgespeichert werden. Weiterhin wird der Ingenieur nach entsprechenden Besprechungen die baulichen Vorgaben und auch die finanziellen Mittel des Kunden erfassen, was ebenfalls personenbezogene Daten sind.

Sobald diese im System automatisiert gespeichert sind, liegt ein datenschutzrechtlicher Verarbeitungsvorgang vor. Dieser muss für seine Rechtmäßigkeit einen entsprechenden Erlaubnistatbestand haben. Der klassische Erlaubnistatbestand im Datenschutzrecht ist die sogenannte Einwilligung des Betroffenen im Sinne von Art. 7 DS GVO. Nach der Vorstellung des Datenschutzrechtes ist jeder Betroffene, also der Inhaber personenbezogener Daten, berechtigt, über diese zu verfügen und damit auch Dritten zu erlauben, solche abzuspeichern. Liegt also eine formgerechte Einwilligung vor, die einerseits elektronisch oder schriftlich erteilt werden kann und andererseits den genauen Zweck der Datenverarbeitung erläutern muss, ist die weitere Verarbeitung personenbezogener Daten unproblematisch möglich, soweit der in der Einwilligung beschriebene Zweck nicht verlassen wird. Erlaubt also ein Kunde die Abspeicherung der Daten zur Bearbeitung des Ingenieurauftrages, liegt hierin nicht gleichzeitig die Erlaubnis, den Kunden mit anderen Produkten des Ingenieurbüros zu bewerben. Dies würde eine Zweckänderung darstellen, die einen neuen Prüfungsvorgang hinsichtlich der Erlaubnis darstellt.

Neben der Einwilligung des Betroffenen gibt aber auch das Gesetz selbst Möglichkeiten für eine rechtmäßige Datenverarbeitung vor, für die keine Einwilligung erforderlich ist. Diese Fälle sind in Art. 6 DSGVO geregelt. Für ein Ingenieurbüro wichtig ist zunächst der in Art. 6 Abs. 1 lit. b DSGVO bezeichnete Rechtfertigungsgrund, nämlich die Datenverarbeitung zur Erfüllung eines vom Betroffenen initiierten Vertrages. Nach dieser Bestimmung kann das Ingenieurbüro ohne Vorliegen einer Einwilligung all diejenigen Verarbeitungsvorgänge vornehmen, die es zur Erfüllung des Ingenieurvertrages benötigt. Dies rechtfertigt einerseits die Erfassung sämtlicher Stammdaten von Kunden des Ingenieurbüros und Bearbeitung des Auftrages und damit auch das Einfließenlassen von Budget und Vorgaben bzw. baulichen Vorstellungen des Kunden in die zu speichernden Kundendaten, andererseits jedoch auch alle Daten, die zur rechnungsseitigen Abwicklung des Vertrages notwendig sind.
Weiterhin darf das Ingenieurbüro alle diejenigen Datenverarbeitungsvorgänge vornehmen, die in Erfüllung eines Gesetzes notwendig sind. Dies kann einerseits im Zusammenhang mit bauordnungsrechtlichen Vorgaben notwendig sein (z. B. Brandschutzkonzept) andererseits aber auch einfache Aufbewahrungsfristen nach dem Handelsgesetzbuch oder der Abgabenordnung betreffen.
Hat ein Ingenieurbüro über diese Gründe hinaus ein berechtigtes Interesse an einer anderen Datenverarbeitung, so darf es diesem berechtigten Interesse nachkommen, wenn dem nicht überwiegende Interessen des Betroffenen entgegenstehen. Diese zunächst sehr sperrig anmutende Bestimmung in Art. 6 Abs. 1 lit. f DSGVO soll am Beispiel der Werbung verdeutlicht werden. Hat man Kundendaten gespeichert und will jetzt die Kunden mit weiteren Leistungen bewerben, hat dies zunächst einmal nichts mit dem ursprünglichen Ingenieurvertrag zu tun. Werbung für künftige Aufträge ist nicht notwendig, um einen abgeschlossenen Vertrag umzusetzen.
Allerdings sieht auch die Datenschutz-Grundverordnung regelmäßig berechtigtes Interesse an Werbung, was in Erwägungsgrund 47 des Gesetzestextes zum Ausdruck kommt. Ein Ingenieurbüro darf also werben, ohne zwingende Einwilligung des Kunden. Es muss dann nur abwägen, ob der Werbung berechtigte Interessen des Kunden entgegenstehen, die das Interesse des Ingenieurbüros an der Werbung überwiegen.

Welche Anforderungen gelten technisch-organisatorisch?

Hat sich der Büroinhaber Gewissheit über die Zulässigkeit der in seinem Unternehmen üblichen Datenverarbeitung verschafft, sind weitere Maßnahmen notwendig. Eine der zentralen weiteren Maßnahmen ist die Erstellung eines technisch-organisatorischen Datenschutzkonzepts. Hier geht es um Fragen der Zugangskontrolle zu Rechnern, welche etwa über einen Passwortschutz gewährleistet wird, sowie um die Zutrittskontrolle zu den Servern des Büros, die zum Teil durch bloßes Abschließen des Serverraums erfolgt. Im Rahmen eines solchen technisch-organisatorischen Konzeptes erarbeitet man also das technische Schutzkonzept. Die sich dabei stellenden Fragen sind zwingend mit der IT-Abteilung bzw. dem beauftragten IT-Unternehmen abzustimmen.

Bei jedem noch so guten technischen Konzept kann es zu Pannen kommen. Solche Datenpannen können etwa der Verlust eines Endgerätes, eines USB-Sticks, eine fehlerhafte Mailversendung oder ein sogenannter Hackerangriff sein. Wird eine solche Datenpanne festgestellt, muss der Inhaber des Ingenieurbüros bzw. der bestellte Datenschutzbeauftragte diese Panne der Datenschutzaufsicht melden, es sei denn, es bestehen keine Risiken für die Personen, deren Daten abhandengekommen sind. Da dies in aller Regel nicht auszuschließen ist, besteht in praktisch allen Fällen eine Meldepflicht gegenüber der Aufsichtsbehörde. Aufsichtsbehörde ist die Landes-Datenschutzbehörde in dem Bundesland, in dem das Ingenieurbüro seinen Sitz hat.
In bestimmten Fällen ist eine Datenpanne auch allen Betroffenen zu melden. Dies ist dann der Fall, wenn hohe Risiken etwa für das Vermögen der Betroffenen drohen, was z. B. bei Abhandenkommen oder Zugänglichmachung von Bankdaten der Fall sein könnte.
Hier sollte das Ingenieurbüro für alle Mitarbeiter einen Maßnahmenplan vorgeben, wie im Falle einer Datenpanne zu verfahren ist. Damit ist in aller Regel gewährleistet, dass es keine unentdeckten, jedoch meldepflichtigen Datenpannen gibt.
Weiterhin arbeiten Ingenieurbüros in aller Regel mit externen Dienstleistern zusammen, die ebenfalls Zugang zu personenbezogenen Daten des Ingenieurbüros (oder deren Kunden bzw. Arbeitnehmern) haben. Solche externen Dienstleister bezeichnet man datenschutzrechtlich als Auftragsverarbeiter. Hier verlangt die Datenschutz-Grundverordnung, dass das Ingenieurbüro sich Gewissheit über die datenschutzrechtlichen Schutzmaßnahmen des Dienstleisters verschafft und mit diesem einen schriftlichen Vertrag abschließt, den man auf der Website der Aufsichtsbehörden herunterladen kann. Mit diesem Vertrag wird sichergestellt, dass der Dienstleister nur nach Weisungen des Ingenieurbüros die fraglichen Daten verarbeitet. Dies sollte auch in regelmäßigen Abständen kontrolliert werden. Typische Dienstleister, die unter diese Bestimmung fallen, sind etwa IT-Dienstleister und Fernwartungsunternehmen, der Steuerberater, der die Lohnbuchhaltung führt, aber auch Letter-Shops, die zur Versendung von Postwurfsendungen an Kunden genutzt werden.

Was gilt beim Arbeitnehmer-Datenschutz?

Neben dem Komplex der Kunden genießt auch der Arbeitnehmer den Schutz der DSGVO. Hier ist es eigentlich relativ unkompliziert: Nach § 26 BDSG neu darf der Inhaber des Ingenieurbüros, also der Arbeitgeber, all diejenigen Vorgänge hinsichtlich der Daten seiner Arbeitnehmer vornehmen, die er zur Begründung, Durchführung und Beendigung eines Arbeitsverhältnisses benötigt. Dies ist neben der Führung der Personalakte natürlich auch die Abwicklung in lohnsteuerlicher Hinsicht bzw. sozialversicherungsrechtlicher Hinsicht.
Arbeitsrechtlich steckt das Problem des Datenschutzes im Detail, so etwa bei der Richtlinie für Endgeräte. ■

Autor
Ralf Wickert
Dornbach GmbH
Rechtsanwaltsgesellschaft, Koblenz

Foto: 123rf/garloon