Praxistipps Datenschutz 06 2017

Ortsbegehungen – wer sich nicht blicken lässt, wird leicht übersehen

Zusammenfassung: Ortsbegehungen sind für Datenschutzbeauftragte unverzichtbar. Wer sich nicht sehen lässt, wird leicht übersehen. Außerdem sind die umfangreichen gesetzlichen Aufgaben von Datenschutzbeauftragten ohne eine Augenscheinnahme vor Ort nicht lösbar. Dokumentation und ein kontinuierlicher Verbesserungsprozess sind als Ergänzungen dringend zu empfehlen.

Die folgenden zehn Ziele machen Begehungen unverzichtbar: Es ist aus mehreren Gründen dringend zu empfehlen, den Stand beim Datenschutz und die Sicherheit von Betriebsgebäuden und Räumen, in denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, anlässlich von Ortsbegehungen zu überprüfen. Dabei geht es bei diesem Thema nicht nur um den Schutz personenbezogener Daten, sondern auch um den Schutz von Betriebs- und Geschäftsgeheimnissen und die Sicherheit allgemein.

Erstens Status prüfen: Anlässlich der Ortsbegehungen kommen Datenschutzbeauftragte und ihre Begleiter vor Ort in die Büros und an die Arbeitsplätze der Beschäftigten. Dort können sie sich durch Augenschein ein genaues Bild vom Stand der Umsetzung von Datenschutz und der IT-Sicherheit sowie anderen zentraler Vorgaben zur Informationssicherheit machen.

Zweitens Geräteausstattung vor Ort abgleichen: Zum zweiten können Angaben zur Geräteausstattung vor Ort mit den Angaben aus der Inventarisierung verglichen werden. Zu den Zwecken der Ortsbegehungen durch den Datenschutzbeauftragten gehört demzufolge auch eine Aufnahme und Begutachtung der Geräte am Arbeitsplatz, mit deren Hilfe personenbezogene Daten erhoben, verarbeitet und genutzt werden. Dies betrifft sowohl stationäre Endgeräte wie PCs, Thin Clients oder IT-Geräte mit erweiterten Funktionen, wie beispielsweise Server, Ausgabegeräte wie fest installierte Telefone, mobile Telefone als Bestandteil der betrieblichen Telefonanlage und dienstliche und private Mobilfunkgeräte wie Handys und Smartphones. Auch Schredder oder Hinweise zur Entsorgung von Datenträgern sind vor Ort besser zu erfassen als remote.

Drittens Übersicht über Umfang der Datenverarbeitung: Dies alles dient allerdings mehr der Übersicht über den tatsächlichen Umfang der Datenverarbeitung als der Kontrolle der Vollständigkeit der Geräte oder der Einhaltung von betrieblichen Vorschriften wie beispielsweise einem Verbot privater Handys am Arbeitsplatz. Alleine schon die Art und Anzahl der Geräte lässt einen tiefen Einblick in die Umsetzung der Prozesse und Verfahren, mit denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, zu. So lässt sich auch vor Ort überprüfen, ob die Inhalte der Verfahrensbeschreibungen tatsächlich aktuell sind. Nicht selten werden bei Ortsbegehungen auch neue Verfahren entdeckt.

Viertens Aufdecken von Risiken: Ein dritter Zweck ist das Aufdecken von Risiken, die zu einem Abfluss personenbezogener oder anderer vertraulicher Daten führen könnte und die Einbindung der Beschäftigten in Lösungsansätze. Ein Beispiel: Im Unternehmen sind Datentonnen für die Entsorgung vertraulicher Unterlagen aufgestellt. Eigentlich sollte es davon genügend Geräte geben. Bei der Ortsbegehung findet der Datenschutzbeauftragte in einem Büro mit mehreren Beschäftigten Plastikkisten mit Unterlagen, die hier so lange aufbewahrt werden, bis „es sich lohnt“ zur Datentonne zu gehen. Da das Büro auch von Besuchern und Reinigungskräften betreten wird, wenn die betroffenen Beschäftigten nicht da sind, kann es sich bei diesem Vorgang um ein erhebliches Risiko für Datenschutz und Informationssicherheit handeln. Ohne Ortsbegehung wäre dem Datenschutzbeauftragten dieses Risiko so nicht bewusst geworden. Zusammen mit den Beschäftigten kann nun nach praktikablen Lösungen gesucht werden.

Fünftens Stoff für Datenschutzunterweisungen: Werden wie soeben beschrieben bei Ortsbegehungen bisher unbekannte Risiken aufgedeckt, ist das auch immer aktueller Stoff für Datenschutzunterweisungen. Oft lässt sich auch zur Veranschaulichung das eine oder andere Bild machen. Hier sollte jedoch stets darauf geachtet werden, dass keine Rückschlüsse auf die Verursacher möglich sein dürfen. Es geht um Vermeidung von Datenschutz- und Sicherheitsvorfällen und nicht um das Bloßstellen einzelner Personen.

Sechstens Bekanntheit des Datenschutzbeauftragten: Vor allem in größeren Unternehmen, in denen sich die Beschäftigen untereinander nicht alle kennen, ist auch der Effekt nicht zu unterschätzen, dass der Datenschutzbeauftragte direkt an den Arbeitsplatz

kommt und der Datenschutz damit ein Gesicht bekommt. Die Hemmschwelle, den Datenschutzbeauftragten bei Fragen zum Datenschutz dann auch tatsächlich anzusprechen, sinkt dadurch beträchtlich. Und: hat der Datenschutz ein Gesicht, sind Verstöße weniger wahrscheinlich als wenn es anonym bleibt.

Siebtens Kontrollen von Arbeitsanweisungen, Richtlinien und Compliance: Vertrauen ist gut, Kontrolle ist besser. Wenn für den Datenschutz und für andere, mit dem Datenschutz zusammenhängende Bereiche verbindliche Vorgaben existieren, müssen diese von Zeit zu Zeit kontrolliert werden. Auch für diesen Zweck sind Ortsbegehungen durch den Datenschutzbeauftragten und andere Verantwortliche unentbehrlich. Werden Abweichungen zu den Vorgaben entdeckt, kann sofort nachgehakt werden, warum das so ist. Gibt es beispielsweise die Vorgabe, dass Unterlagen mit personenbezogenen Daten verschlossen aufzubewahren sind, kann diese naturgemäß nicht umgesetzt werden, wenn keine abschließbaren Schränke oder Bürocontainer vor Ort sind. Solche Details können Datenschutzbeauftragte am besten selbst vor Ort erfragen.

Achtens Prüfpflichten des Datenschutzbeauftragten erfüllen: Zu den beiden Hauptaufgaben von Datenschutzbeauftragten gehört auch die Prüfung, ob Systeme der Datenverarbeitung datenschutzkonform betrieben werden. Dies ist auch mit Ortsbegehungen verbunden. Es ist nicht vorstellbar, dass diese Kontrollpflicht ohne den eigenen Augenschein vor Ort durchgeführt werden kann. Selbst wenn Datenschutzbeauftragte über Hilfspersonal wie Datenschutzkoordinatoren verfügen, und diese entdecken Unstimmigkeiten, kommen Datenschutzbeauftragte normalerweise nicht ohne eigenen Augenschein zu einem unabhängigen Urteil.

Neuntens Vorbereitungen von externen Audits: Wenn im Unternehmen von Zeit zu Zeit oder auch regelmäßig externe Audits stattfinden, beispielsweise im Zusammenhang mit der Auftragsdatenverarbeitung als Auftragnehmer oder mit Zertifizierungen, Überwachungsaudits und Rezertifizierungen, sollten im Vorfeld immer wieder Ortsbegehungen durchgeführt werden.

Zehntens Synergieeffekte nutzen: Ortsbegehungen müssen zu unterschiedlichen Zwecken durchgeführt werden. Diese können unter anderem zu Zwecken der Arbeitssicherheit und des Brandschutzes erfolgen. Um Synergieeffekte zu nutzen, können diese Begehungen zusammen mit den Begehungen zu Zwecken des Datenschutzes durchgeführt werden. So werden die Beschäftigten nicht mehrfach in ihren Arbeitsabläufen unterbrochen.

Adressaten: Ortsbegehungen Datenschutz sowie deren Auswertungen sind eine wichtige Informationsquelle für eine Vielzahl von Adressaten. An erster Stelle steht natürlich das Interesse des Datenschutzbeauftragten an Ortsbegehungen, denn diese sind ein wichtiger Bestandteil seiner Aufgaben. An den Ergebnissen interessiert muss auch die Geschäftsführung sein, zumindest dasjenige Mitglied der Geschäftsführung, das für die Sicherheit im Unternehmen zuständig ist. Ein vitales Interesse an den Ergebnissen haben auch der IT-Sicherheitsbeauftragte sowie die Hausverwaltung (Facility Management). Falls ein Betriebsrat vorhanden ist, so ist dieser sicher auch an den Ergebnissen der Ortsbegehungen interessiert, zumindest in den Bereichen wie der Organisation der Beschäftigtendaten, die zu den Bereichen gehören, für die der Betriebsrat laut Betriebsverfassungsgesetz eine Kontrollpflicht hat. Weitere Adressaten wie IT-Leitung, Personalleitung, Vertriebsleitung usw. gehören ebenfalls zu den Adressaten der Ortsbegehungen Datenschutz.

Dokumentation: Ortsbegehungen sollten dokumentiert werden. Dazu gehört die grobe Beschreibung der Örtlichkeiten, beispielsweise in welchem Stockwerk das jeweilige Büro liegt, welche Funktion vorliegt (Büro, Serverraum, Technikraum, Archiv usw.), wie viele Arbeitsplätze mit und ohne IT-Ausstattung im Büro vorhanden sind, welches die höchste Schutzstufe der dort erhobenen, verarbeiteten und genutzten personenbezogenen Daten vorliegt und welche Schutzmaßnahmen bereits ergriffen wurden, ob im jeweiligen Raum Publikumsverkehr (intern und extern) erfolgt, welche offenkundigen Risiken zu beobachten sind und ob die Unterlagen mit Personenbezug verschlossen aufbewahrt werden können.

Auswertungen: Die anlässlich der Ortsbegehungen dokumentierten Ergebnisse sind Grundlage für eine Auswertung. Hierin wird zum einen dokumentiert, welche Situation die Auditoren bei den Ortsbegehungen vorgefunden haben. Falls Mängel festgestellt werden, müssen hierzu Handlungsempfehlungen in die Auswertung einfließen. In die Erstellung dieser Handlungsempfehlungen sollten die betreffenden Beschäftigen in den jeweiligen Arbeitsräumen eingebunden werden, was die Bereitschaft zur Umsetzung deutlich erhöht. Die Handlungsempfehlungen können in Arbeitsanweisungen, Richtlinien, Betriebsvereinbarungen oder Compliance-Regeln einmünden, wenn die Verantwortlichen dies entsprechend anordnen. Der Charakter der Ortsbegehungen

bringt es mit sich, dass diese Auswertungen für jeden analysierten Arbeitsraum anders aussehen können. Werden verbindliche Regelungen erstellt, so sind diese mittels Schulungsmaßnahmen zu erläutern und in der Folge auch zu kontrollieren.

Wiederholungen: Ortsbegehungen sollten wiederholt werden. Anfangs empfiehlt sich eine Vorankündigung, schließlich geht es nicht um ein „Vorführen“. Später, vor allem nach Anordnung spezieller Maßnahmen, sollten auch unangekündigte Kontrollen erfolgen.

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de