Wie werden die Kundendaten im Büro sicher(er)?

Vortrag auf der Fachtagung des IVD Mitte-Ost

21.03.2024

Sven R. Johns

Rechtsanwalt

Externer Datenschutzbeauftragter

Datenschutzauditor (Bitkom)

sven.johns@mosler-partner.com

Kunden lieben Datenschutz

Google
Think with Google
September 2022

T

Think with Google DACH <thinkwithgoogle-noreply@google.com>
An: sven@sven-johns.de

Im Webbrowser ansehen

Nutzerinnen und Nutzer legen großen Wert auf Datenschutz. Und das sollten Werbetreibende umso mehr

Links sitzt eine Frau mit einem Smartphone in der Hand auf einem großen grauen unverschlossenen Vorhängeschloss. Rechts sitzt eine Frau auf einem großen grünen verschlossenen Vorhängeschloss und arbeitet an einem Laptop.

Wenn Nutzerinnen und Nutzer den Datenschutz eines Unternehmens als mangelhaft empfinden, kann sich das fast so negativ auswirken wie eine tatsächliche Datenpanne. Eine neue Studie von Google und Ipsos mit über 20.000 Teilnehmenden hat gezeigt, wie viel für Marken in puncto Datenschutz auf dem Spiel steht. Lesen Sie, mit welchen Praktiken Sie Ihren Nutzerinnen und Nutzern ein

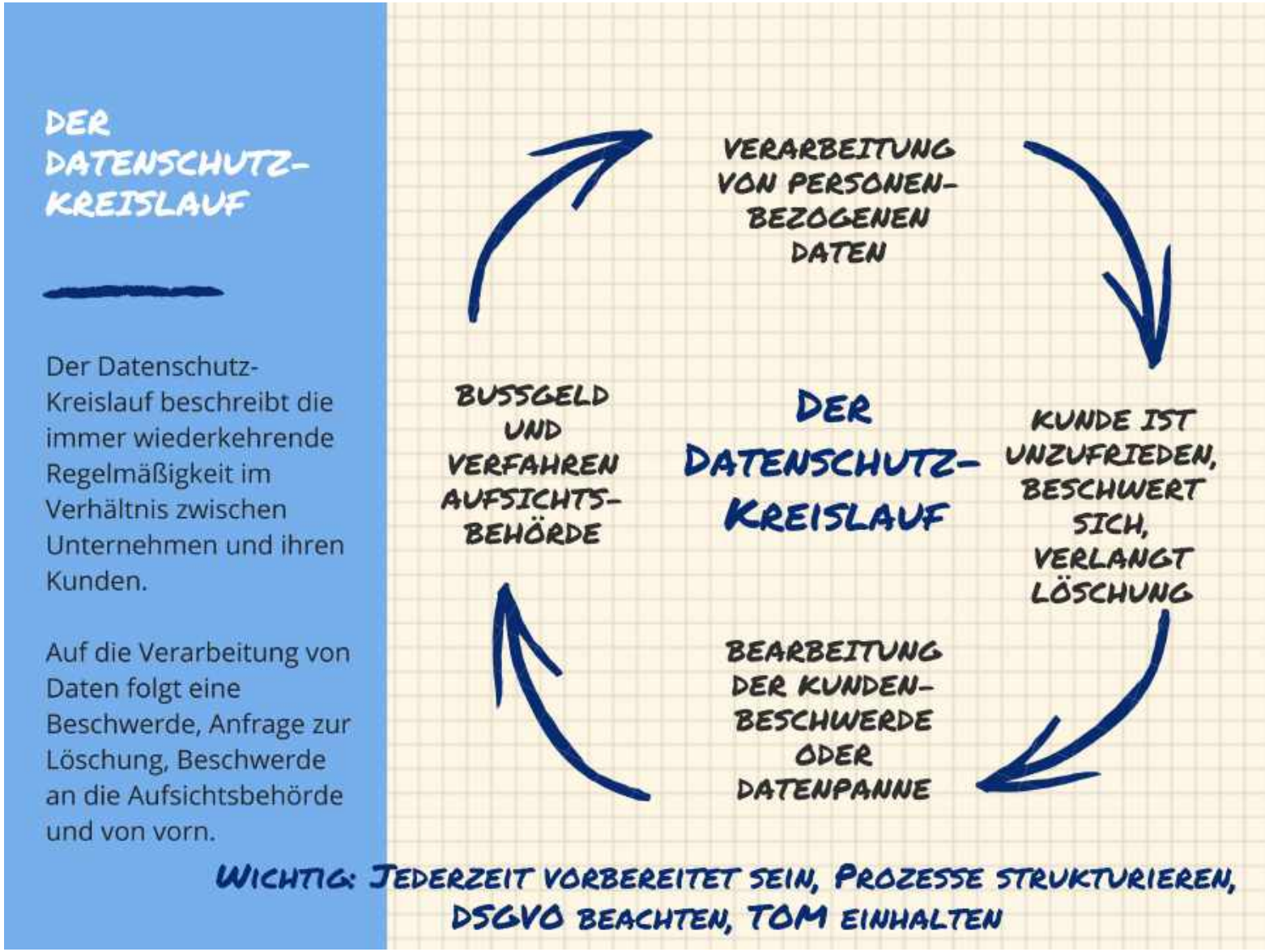
Quelle:
Google
09/2022

Datenschutzpraktiken, die zu einem Gefühl der Kontrolle beitragen

Quelle: Google/Ipsos, Frankreich, Deutschland, Niederlande, Schweden, Großbritannien. „Privacy by design: the benefits of putting people in control". n=10.001. Online-Umfrage unter Teilnehmenden zwischen 18 und 70 Jahren, Juli 2022. Frage: Inwiefern hatten Sie in dem gerade durchgespielten Szenario das Gefühl, die Kontrolle über die Daten zu haben, die sie mit (Namen der Marke) teilen?

Wann werden wir
als DSB eingeschaltet?

Sehr häufig nach
Kundenbeschwerden



MAKLERBÜROS

Übersicht Bußgelder

5000,- EUR Verstöße gegen MaBV

15.000,- EUR Verstöße nach GEG

1 Mio. EUR Verstöße nach GwG

20 Mio. EUR Verstöße nach DSGVO

Für Immobilienfirmen von www.datenschutz.immobilien

Die Sicherheit der Kundendaten in den Immobilienbüros

Welche Daten haben wir in unseren Büros? Welche Daten sind für Täter interessant?
(dahinterstehende Frage: Welche Risikodisposition besteht im Unternehmen)

- Kontodaten – Mietverwaltung, Maklerbüro, Mitteilung an Notar für Notarvertrag
- Personalausweiskopien – Identitätsdiebstahl
- E-Mail-Adressen – zur Weiterleitung von Schadsoftware (Maklerbüro mit 15.000 Adressen, die leicht erbeutet werden können, ist ein lohnendes Ziel)

Konkrete Beispiele für Gefährdung und Schäden in Immobilienbüros aus meiner Paxis

Hausverwaltung – Ransomwareangriff – alle Daten verschlüsselt – kein Zugang zu Buchhaltung/Mieterdaten/Eigentümerdaten etc. – Lösegeldforderung – wollte nicht bezahlen – was nun?

Maklerbüro – ca. 15.000 Kundendaten in der CRM – Ein MA klickt auf einen falschen Link – Zugang zum Microsoft365-Konto – sowohl alle dort abgelegten Dokumente als auch alle dort abgelegten Kundendaten – plus Zahlungsdaten des Unternehmens für das Abo

Maklerbüro – E-Mail an Kunden mit einem Link, hinter dem sich Schadsoftware verbirgt, Versand an mindestens 150 Kunden (soweit erkennbar) – Folge: Prüfung, ob Infizierung des eigenen Netzwerks, hohe Kosten für IT-forensische Maßnahmen

Maklerbüro – Täter scheibt an Kunden mit einem „neuen“ Angebot an – hinter dem Link/Anlage liegt eine Schadsoftware – Täter hat dafür eine eigene domain angelegt, die fast ähnlich klingt wie die eigentliche domain

Wie sieht das nun konkret in den Büros aus?

Identifikationspflicht beim Immobilienkauf (aus: Tätigkeitsbericht Aufsicht Sachen Datenschutz 2022)

Ein Kaufinteressent wurde in einem Immobilienportal auf eine interessante Immobilie aufmerksam. Sodann richtete er eine schriftliche Anfrage an den Immobilienmakler, der das Objekt inserierte. Schnell war ein Besichtigungstermin vereinbart, allerdings forderte das Maklerunternehmen zuvor eine beiderseitige Kopie des Personalausweises von dem potenziellen Kaufbewerber. Zur Begründung fügte der Makler seiner E-Mail-Nachricht eine Erklärung zum Geldwäschegesetz und auch einen Zeitungsbericht bei, der die Pflicht zur Identitätsprüfung zum Gegenstand hatte. Es gelang ihm augenscheinlich nicht, den Kaufinteressenten damit zu überzeugen, sodass sich dieser schließlich mit einer Beschwerde an meine Behörde wandte.

Bei einer Transaktion, wie dem Verkauf eine Wohnimmobilie, ist die Maklerin bzw. der Makler verpflichtet, vor deren Durchführung seine Vertragspartner zu identifizieren (§ 11 Abs. 1 GwG). Im Umkehrschluss haben die Vertragspartner diesem die Informationen und Unterlagen zur Verfügung zu stellen, die dieser zur Identifizierung benötigt (§ 11 Abs. 6 Satz 1 GwG). Um die Identifikationspflicht auszulösen, bedarf es allerdings eines ernsthaften Interesses (§ 11 Abs. 2 GwG), wovon zum Zeitpunkt der Objektbesichtigung noch nicht auszugehen ist.

Wie sieht das nun konkret in den Büros aus?

Identifikationspflicht beim Immobilienkauf

Zur Identifikation hat sich die bzw. der Verpflichtete von beiden Vertragsparteien einen gültigen amtlichen Ausweis (Pass, Personalausweis oder Pass/Ausweisersatz) zeigen zu lassen (§ 12 Abs. 1 Satz 1 Nr. 1 GwG).

Das Geldwäschegesetz regelt auch im Einzelnen, welche Daten von natürlichen Personen zum Zweck der Identifikation zu erheben sind (§ 11 Abs. 4 Nr. 1 GwG). Demnach fallen hierunter neben Vor- und Nachname auch Geburtsdatum und -ort, die Staatsangehörigkeit sowie die Wohnanschrift. Ebenso wie die Art, die Nummer und die den Ausweis ausstellende Behörde sind alle erhobenen Daten aufzuzeichnen (§ 8 Abs. 1, Abs. 2 Satz 1 GwG). Von dem Ausweisdokument muss die bzw. der Verpflichtete zudem eine vollständige Kopie anfertigen oder dieses vollständig optisch digital erfassen (§ 8 Abs. 2 Satz 2 GwG). Die erhobenen Angaben und eingeholten Informationen sind dann für einen Zeitraum von mindestens fünf Jahren aufbewahren (§ 8 Abs. 4 Satz 1 GwG).

Die datenschutzrechtliche Zulässigkeit resultiert damit aus der oder dem Verpflichteten jeweils auferlegten gesetzlichen Pflichten (Art. 6 Abs. 1 Unterabs. 1 Buchst. c, Abs. 2 DSGVO). Was die Anfrage des potenziellen Immobilienkäufers angeht, so waren dessen Zweifel unterm Strich berechtigt. Ich konnte ihm hierzu noch ergänzende rechtliche Erläuterungen geben und die maßgeblichen Rechtsvorschriften benennen.

Die Notfallkarte
als erste Sofortmaßnahme
bei einer Cyber-Attacke

Quelle: BSI

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden

Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen	Beobachtungen dokumentieren	Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Tätigkeitsbericht Aufsicht Sachen Datenschutz 2022

Fehlversendung

Nach wie vor stellt die Fehlversendung von Unterlagen mit personenbezogenen Daten mit ca. einem Drittel der Meldungen von Datenschutzverletzungen die häufigste Fallgruppe dar. Dem liegt in der Regel ein unbeabsichtigter Versand zugrunde, welcher auf falsche Zuordnung von Unterlagen, fehlerhafte maschinelle Kuvertierung, falsche Adressdaten oder schlicht auf Namensverwechslung zurückzuführen ist.

Offener E-Mail-Verteiler

Ebenfalls ist der sogenannte offene E-Mail-Verteiler, bei welchem die E-Mail-Adressen nicht in das Blindkopie-Feld (bcc), sondern in der Regel versehentlich in das Kopie-Feld (cc) eingetragen werden, eine typische Fallgruppe der Datenschutzverletzungen, die bei mir gemeldet werden. Der offene E-Mail-Verteiler ist dann meldepflichtig, wenn die E-Mail-Empfänger/innen mit der offenen Verbreitung ihrer E-Mail-Adresse nicht ausdrücklich einverstanden waren, da es dann an einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten mangelt.

Einbruch und Diebstahl

Datenschutzverletzungen im Rahmen von Diebstählen und Einbrüchen stellen ebenfalls auch in diesem Berichtszeitraum eine typische Fallgruppe dar, welche bei mir gemeldet wurde.

Cyberkriminalität

Typische Fälle im Bereich der Cyberkriminalität sind Spam- und Phishing-Mails, die Verschlüsselung von Systemen mit Ransomware oder allgemein die Verwendung von Schadsoftware (Malware) bzw. das Ausnutzungen von Schwachstellen. Zur Vermeidung von Meldefällen ist hinsichtlich der technisch-organisatorischen Maßnahmen stets besonderes Augenmerk auf die Informations/Datensicherheit zu legen.

Die Technischen und organisatorischen Maßnahmen im Unternehmen

Aufsicht Datenschutz – Tätigkeitsbericht

Bereich Bauen und Wohnen - teilweise Beschäftigte verstärkt sensibilisiert werden müssten, da es sich in vielen Fällen um menschliches Fehlverhalten handelte. Erwähnenswert sind hier häufige Fälle des Fehlversandes von Protokollen, Mietangeboten, Interessent:innenbögen, Wirtschaftsplänen, Kündigungs- und Mietänderungsschreiben.

…

In diesem Kontext weisen wir auf die Wichtigkeit umfassender technischer sowie organisatorischer Maßnahmen hin, die das Erstellen und Versenden von Kund:innenschreiben in datenschutzkonformer Weise ermöglichen. Vor Versand der Schreiben empfahlen wir zusätzlich die Sichtung der Schreiben im Vier-Augen-Prinzip, um das Risiko für Datenschutzverletzungen dieses Ausmaßes zu verringern.

Die Technischen und organisatorischen Maßnahmen im Unternehmen

Aufsicht Bayern, aktueller Tätigkeitsbericht – Beispiele unzureichende TOM

- Veröffentlichung auf Grund von Unwissenheit oder mangelnder Sensibilität, dass ein personenbezogenes Datum nicht veröffentlicht werden darf: Im Berichtszeitraum wurde beispielsweise ein Gemeinderatsprotokoll auf die Webseiten einer Gemeinde eingestellt, in dem Gesundheitsdaten einer Person enthalten waren, die durch die genannte Amtsbezeichnung identifizierbar war.

- Veröffentlichung auf Grund von Unachtsamkeit: Im Berichtszeitraum wurden beispielsweise nicht für die Öffentlichkeit bestimmte Dokumente aus einer Gemeinderatssitzung versehentlich auf den Webseiten der Gemeinde veröffentlicht, die zugleich personenbezogene Daten von Bürgerinnen und Bürgern enthielten.

- Veröffentlichung auf Grund der falschen Konfiguration eines Webservers: Auch beispielsweise zu weit reichende Berechtigungen für interne Verzeichnisse zum Datenaustausch können zur unzulässigen Veröffentlichung führen.

Die Technischen und organisatorischen Maßnahmen im Unternehmen

Aufsicht BW, aktueller Tätigkeitsbericht – Beispiele unzureichende TOM

Bei der Frage, welche technischen und organisatorischen Maßnahmen zu treffen sind, hat der Verantwortliche kein Entschließungsermessen, jedoch im Rahmen der Vorgaben der DS-GVO ein Auswahlermessen. Er hat so betreffend der durch die Verarbeitung entstehenden Risiken für die Rechte und Freiheiten betroffener Personen mit risikoadäquaten Maßnahmen ein angemessenes Schutzniveau zu treffen

Die Technischen und organisatorischen Maßnahmen im Unternehmen – aktuelles Bußgeld

Unzureichende technische und organisatorische Maßnahmen

Kunde der Caixabank S.A. hatte Zugriff auf einen Zahlungsnachweis einer unbekannten Person an eine weitere ihm unbekannte Person erhalten. Darin enthalten: Namen des Senders und des Empfängers, die Wohnadresse, IBAN der Konten sowie Herkunfts- und Zielort der Überweisung.

Keine ausreichende Auskunft der Bank an den Kunden -> Beschwerde

Feststellungen: keine ausreichenden TOM bei der Bank, keine datenschutzfreundlichen Voreinstellungen der Technik im Sinne von Art. 25 DSGVO, kein spezifisches Verfahren für die Bearbeitung von Kundenanfragen auf dem Gebiet des Datenschutzes eingerichtet

Bußgeld in Höhe von 5.000.000 Euro.

-> Verantwortliche müssen a) geeignete technische und organisatorische Maßnahmen treffen b) die Rechte der Betroffenen zu schützen und c) die Anforderungen der DSGVO d) Gestaltung von Unternehmensprozessen datenschutzkonform angehen e) Prozesse einrichten, die die Rechte betroffener Personen angehen

Die Technischen und organisatorischen Maßnahmen im Unternehmen

Art. 32 DSGVO

Grundsätze der Datenverarbeitung gem. Art 5

Aufstellung TOM nutzen und bearbeiten

Einmal im Jahr überprüfen

Liste erstellen

Gemeinsam mit IT-Beratung und DSB ausfüllen und aktualisieren

TOM sind kein Dokument für Dritte, nur für den internen Gebrauch und zur Vorlage bei der Aufsicht Datenschutz, wenn von dort angefordert

Risikoüberprüfung = Ziel der TOM

Risiken - ob unbeabsichtigt oder unrechtmäßig –

- Vernichtung
- Verlust
- Veränderung
- unbefugte Offenlegung von beziehungsweise
- unbefugten Zugang zu personenbezogenen Daten

die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Empfehlungen der Aufsicht Datenschutz zu den TOM

Empfehlungen der Aufsicht Datenschutz zu den TOM

Das Bayerische Landesamt für Datenschutzaufsicht gibt in seinen Empfehlungen konkrete Hinweise zur Umsetzung und Überprüfung der technischen und organisatorischen Maßnahmen (TOM) nach Art. 32 DSGVO. Hier einige der Empfehlungen:

1. **Risikoanalyse**: Unternehmen sollten eine regelmäßige Risikoanalyse durchführen, um die relevanten Risiken für die Verarbeitung personenbezogener Daten zu identifizieren. Auf Basis der Risikoanalyse können dann geeignete TOM ausgewählt werden.
2. **Dokumentation**: Die TOM sollten dokumentiert und regelmäßig überprüft und aktualisiert werden. Dabei sollte auch festgehalten werden, wer für die Umsetzung der TOM verantwortlich ist.
3. **Schulung und Sensibilisierung**: Mitarbeiter sollten regelmäßig geschult und sensibilisiert werden, um ein Bewusstsein für den Datenschutz und die Bedeutung der TOM zu schaffen.
4. **Testen und Überprüfen**: Die TOM sollten regelmäßig getestet und überprüft werden, um ihre Wirksamkeit sicherzustellen. Dazu können beispielsweise Penetrationstests oder Sicherheitsaudits eingesetzt werden.

Empfehlungen der Aufsicht Datenschutz zu den TOM

5. Notfallplanung: Unternehmen sollten einen Notfallplan für den Fall eines Datenschutzvorfalls oder einer Sicherheitslücke entwickeln und diesen regelmäßig überprüfen und aktualisieren.

6. Auftragsverarbeitung: Bei der Auftragsverarbeitung sollten Unternehmen darauf achten, dass auch ihre Auftragsverarbeiter geeignete TOM umsetzen. Hier sollten entsprechende Vereinbarungen getroffen und überprüft werden.

7. Evaluierung: Unternehmen sollten regelmäßig evaluieren, ob ihre TOM noch angemessen und ausreichend sind. Dabei sollten auch Änderungen im Unternehmen oder in der IT-Landschaft berücksichtigt werden.

Was ist Technik und was ist Organisation?

Technik

Geräte

Server

Mobile Endgeräte

IT

Backups

Organisation

Verantwortlichkeit Geschäftsleitung

Regelungen (Prozesse, Arbeitsanweisungen etc.) treffen

Handreichungen, Anweisungen, Betriebsvereinbarungen, Festlegungen, Ergänzungen zum Arbeitsvertrag

Organisation – bürointern mit den Mitarbeitenden

Folgende Regelungen sollten Immobilienfirmen treffen:

Festlegungen zum Umgang mit pbD im Unternehmen
Festlegung private Nutzung E-Mail-Accounts
Festlegung private Nutzung Internet am Arbeitsplatz
Remote-Arbeitsplatz-Richtline
Vorgang Meldung von Datenpannen
VPN-Nutzung vorschreiben
Nutzungs- und Rollenkonzept erstellen (wer hat Zugriff auf welche Daten?)
Schulungskonzept
Liste TOM erstellen und aktualisieren
Empfehlungen Passwortvergabe, Passwortmanager einsetzen

Vorbeugende Maßnahmen – Tätigkeitsbericht Aufsicht Datenschutz Sachsen

Daten sichern!

Die Daten von Firmen und Organisationen müssen unbedingt gesichert sein. Sichere OfflineDatensicherungen sollten so verwahrt werden, dass sie selbst nicht von Cyberangriffen erfasst werden können.

Firewall richtig konfigurieren!

Die Firewall sollte nur erforderliche Datenverbindungen zulassen. Auch ein Frühwarnsystem über ungewöhnlich hohen Datenverkehr kann Systemverantwortlichen dabei helfen, Datenabflüsse zu erkennen und so größeren Schaden abzuwenden.

Notfallplan beachten!

Für die Fälle von Cybererpressungen bzw. Hacker-Angriffen sollte ein Notfallplan vorliegen, der im Akutfall abzuarbeiten ist. Dazu gehört auch eine Regelung, wann der IT-Administrator, interne Datenschutzbeauftragte, die Datenschutzaufsichts- behörde oder auch die Mitarbeiter, Unternehmensleitung und Kunden zu informieren sind.

Vorbeugende Maßnahmen – Tätigkeitsbericht Aufsicht Datenschutz Sachsen

Reservetechnik vorhalten!

Eine dringende Empfehlung ist zudem, Reservetechnik vorzuhalten. Ermittler können so das angegriffene IT-System forensisch sorgfältig untersuchen, während das Unternehmen trotz Cyberangriff rasch wieder arbeitsfähig ist.

Frühzeitig kommunizieren!

Verantwortliche sollten betroffene Personen oder Abteilungen auch dann schnell über den Vorfall informieren, wenn noch nicht sicher ist, ob und welche personenbezogene(n) Daten betroffen sind.

Weiterbildung!

IT-Verantwortliche und all jene, die in Unternehmen und Organisationen für die Informationssicherheit zuständig oder am jeweiligen Prozess beteiligt sind, benötigen regelmäßig Weiterbildung.

Was ist Technik und was ist Organisation?

Technische Schutzmaßnahmen

Die Geräte müssen über einen aktuellen Anti-Viren-Schutz und eine aktuelle Firewall verfügen.

Die Geräte müssen passwortgesichert sein. Das Passwort sollte Zahlen sowie eine Kombination aus Groß- und Kleinbuchstaben enthalten. Es sollte auch nicht zu kurz sein.

Sofern Dritte wie Familienangehörige ebenfalls das Gerät benutzen, müssen Ordner mit personenbezogenen Daten passwortgesichert sein, so dass sie für Dritte nicht zugänglich sind.

Die Weitergabe von Daten sollte verschlüsselt erfolgen. Verschlüsselungssoftware ist zu installieren und zu benutzen. Sofern Dienstleister Dokumentenmanagementsysteme zum Hochladen von Dateien und zur Kommunikation anbieten, die mit Benutzerkonto und individuellem Passwort gesichert sind, sollten diese genutzt werden. Sofern möglich, sollten Daten in anonymisierter oder pseudonymisierter Form weitergebeben werden.

Was ist Technik und was ist Organisation?

Von den Dateien sind regelmäßig Sicherheitskopien zu erstellen. Dabei sind die Löschpflichten zu beachten. Daher sollten die Datenträger regelmäßig überschrieben werden.

Akten mit personenbezogenen Daten sind so aufzubewahren, dass Dritte keinen ungehinderten Zugang erhalten. Dies kann durch verschließbare Aktenschränke oder durch Abschließen des Raumes geschehen. Auch ausgedruckte E-Mails und Briefe dürfen nicht offen herumliegen.

Bei der Benutzung von Mailverteilern gilt: E-Mailadressen der anderen Empfänger dürfen nicht sichtbar sein (bcc-Einstellungen); nur verschlüsselte W-LANs sollten genutzt werden.

Akten sind bei Ablauf der Löschfristen ordnungsgemäß durch den Einsatz von Aktenvernichtern oder durch Dienstleister zu vernichten. Auch Datenträger und Computer sind, nachdem sie aussortiert wurden, ordnungsgemäß zu löschen, beispielsweise durch Einsatz von professioneller Überschreibungssoftware.

Etwaiges Reinigungspersonal ist sorgfältig auszuwählen.

Wie hoch ist der Zeitaufwand?

Der geschätzte Zeitaufwand für diese Implementierungsmaßnahmen hängt von der Größe der Firma, der Art und Menge der personenbezogenen Daten und der Komplexität der IT-Systeme ab.

Rechnen Sie damit, dass es einige Wochen bis mehrere Monate dauern kann, um alle erforderlichen Maßnahmen umzusetzen.

Wichtig ist, dass **die IT-Beratung** und der **externe Datenschutzbeauftragte**, sofern dieser vorhanden ist, einbezogen werden. Dadurch kann ein wesentlicher Teil des Zeitaufwands reduziert werden.

Empfehlung: Vernachlässigen Sie diese Maßnahmen nicht und nehmen sich die Zeit, um sicherzustellen, dass alle personenbezogenen Daten angemessen geschützt werden.

Die Nichteinhaltung der TOM ist ein Verstoß gegen die Anforderungen der DSGVO und kann mit einem Bußgeld geahndet werden. Die Bußgeldvorschriften finden Sie in Art. 82 der DSGVO. Die Bußgeldandrohung reicht bis zu 20 Mio. EUR Bußgeld.

Vorschlag für die Vorgehensweise in Immobilienfirmen

1. **Die Identifizierung der personenbezogener Daten:** Das Unternehmen muss zuerst alle personenbezogenen Daten, die es verarbeitet, identifizieren und dokumentieren. Dies kann Kunden- und Vertragsdaten, aber auch Mitarbeitendendaten und andere interne Daten umfassen.

Identifizierung der Daten

- Käuferdaten
- Verkäuferdaten
- Interessentendaten
- Partner/Kooperationspartnerdaten
- Adressdaten
- Objektdaten
- Grundbuchangaben
- Wertermittlung
- Finanzierungsunterlagen
- Zusammenarbeit mit Kollegen
- (freie) Mitarbeitendendaten …
- (vgl. die Angaben aus dem Informationsschreiben nach Art. 13 und 14 DSGVO)

Vorschlag für die Vorgehensweise in Immobilienfirmen

2. Die Durchführung einer Risikobewertung: Die Immobilienfirma muss eine Risikobewertung durchführen, um potenzielle Bedrohungen und Schwachstellen in Bezug auf die Verarbeitung personenbezogener Daten zu identifizieren. Hier können verschiedene Methoden verwendet werden. Eine der Methoden, die in der DSGVO genannt werden, ist die Datenschutzfolgenabschätzung (DSFA). Auch ein Datenschutzaudit kann hierzu beitragen.

Durchführung einer Risikoanalyse der TOM

Eine wirkungsvolle Risikoanalyse der technischen und organisatorischen Maßnahmen (TOM) in einem Unternehmen kann wie folgt erfolgen:

1. Schritt: **Identifikation von Datenkategorien und -quellen** - Es müssen alle personenbezogenen Daten identifiziert werden, die in der Firma verarbeitet werden. Hierbei sollten die Datenkategorien (z.B. Kunden-, Mitarbeiter-, Lieferanten- oder Bewerberdaten) und die Datenquellen (z.B. E-Mail-System, Buchhaltungssoftware oder Personalverwaltungssystem) erfasst werden.
2. Schritt: **Festlegung der Verarbeitungszwecke** - Es sollten alle Verarbeitungszwecke der personenbezogenen Daten erfasst und dokumentiert werden, um später mögliche Risiken bewerten zu können.
3. Schritt: **Identifikation von Bedrohungen** - Es müssen mögliche Bedrohungen und Gefahren für die personenbezogenen Daten erkannt werden, die in der Firma verarbeitet werden können. Beispiele hierfür sind Diebstahl von Hardware oder Daten, Hackerangriffe oder menschliches Fehlverhalten.
4. Schritt: **Bewertung der Risiken -** Die erkannten Bedrohungen und Gefahren müssen bewertet werden, um das Risiko einschätzen zu können. Hierbei sollten die Wahrscheinlichkeit und die Auswirkungen eines Datenschutzvorfalls berücksichtigt werden.
5. Schritt: **Auswahl geeigneter Maßnahmen** - Es müssen geeignete technische und organisatorische Maßnahmen ausgewählt werden, um das identifizierte Risiko zu minimieren. Die Maßnahmen sollten entsprechend der Risikobewertung priorisiert werden.
6. Schritt: **Dokumentation und Überprüfung** - Alle Schritte der Risikoanalyse und die daraus abgeleiteten Maßnahmen sollten dokumentiert und regelmäßig überprüft und aktualisiert werden.

.

Mehrfachverarbeitung von Daten? Unterschiedliche Verarbeitungsorte für gleiche Vorgänge

- - - Wir nutzen „parallele“ Systeme - - -

E-Mail vs. Postverkehr

E-Mail-Hauptprogramm vs. E-Mail-Client

Kundenakten in der Software vs. Papierakten

Kundendaten in der Software vs. Kundendaten im Outlook-Adressbuch

Digitale Exposees vs. Papierexposees

Digitale Besichtigungen vs. Besichtigungsprotokolle

E-Mail-Funnel für die Akquisition vs. Postverteiler für Mailings

Vorschlag für die Vorgehensweise in Immobilienfirmen

3. **Die Implementierung geeigneter technischer und organisatorischer Maßnahmen**: Basierend auf der Risikobewertung müssen geeignete technische und organisatorische Maßnahmen implementiert werden, um personenbezogene Daten zu schützen. Dazu können Verschlüsselung, Zugriffskontrollen, regelmäßige Backups, sichere Datenübertragungen und andere Sicherheitsmaßnahmen gehören.

Rollen- und Berechtigungskonzept = Zugangsberechtigtung

Sicherstellen, dass jeder Mitarbeiter nur die Daten und Ressourcen zugreifen kann, die für seine Arbeit notwendig sind.
= Risiko von unberechtigtem Zugriff auf personenbezogene Daten minimieren

1. Bestandsaufnahme aller Nutzer und ihrer Zugriffsrechte auf personenbezogene Daten durchführen. Verschiedenen Rollen innerhalb des Unternehmens identifizieren und festlegen. Welche Daten zu welchem Zeitpunkt benötigt, um den Geschäftsprozess nicht zu behindern.

2. Basis dieser Bestandsaufnahme = Entwicklung Rollen- und Berechtigungskonzept = genaue Beschreibung - nicht zu allgemein definieren

3. In der Software: auf vorhandene Funktionen zur Zugriffskontrolle zurückgreifen. - Berechtigungen regelmäßig überprüfen und anpassen

4. Überprüfung der Wirksamkeit = in regelmäßigen Abständen Zugriffskontrollprüfung durchführen

Bußgeld verhängt, weil Insolvenzverwalter im Rahmen der insolvenz die Zugangsberechtigungen von (ehemaligen) Mitarbeitednen nicht gesperrt/verändert hat.

Hinweise zu einer wirkungsvollen Datensicherung

Um eine effektive Datensicherung im Jahr 2024 sicherzustellen, gibt es verschiedene Empfehlungen und Maßnahmen, die ergriffen werden können. Der neueste Stand der Technik beinhaltet:

1. **Regelmäßige Datensicherungen** - Es ist empfehlenswert, regelmäßige Datensicherungen durchzuführen, um bei Datenverlusten schnellstmöglich auf eine Sicherungskopie zurückgreifen zu können. Dabei sollte darauf geachtet werden, dass sowohl die Häufigkeit als auch die Art der Datensicherung den individuellen Bedürfnissen des Unternehmens entsprechen.
2. **Einsatz von Cloud-basierten Backup-Lösungen** - Cloud-basierte Backup-Lösungen bieten eine sichere und zuverlässige Möglichkeit, um Daten zu sichern. Hierbei sollten jedoch die Datenschutzbestimmungen sowie die Sicherheitsvorkehrungen des Cloud-Anbieters genau überprüft werden.
3. **Verschlüsselung von Backups** - Es ist empfehlenswert, alle Datensicherungen zu verschlüsseln, um sicherzustellen, dass die gesicherten Daten bei Verlust oder Diebstahl nicht in die falschen Hände geraten.
4. **Redundante Datensicherungen** - Eine redundante Datensicherung bietet zusätzlichen Schutz, indem mehrere Kopien von wichtigen Daten an verschiedenen Orten gespeichert werden.
5. **Überprüfung der Datensicherungen** - Es ist wichtig, regelmäßig zu überprüfen, ob die Datensicherungen ordnungsgemäß funktionieren und ob alle wichtigen Daten gesichert wurden.
6. **Einhaltung von gesetzlichen Anforderungen** - Es sollte darauf geachtet werden, dass die Datensicherung den gesetzlichen Anforderungen entspricht, wie beispielsweise der Datenschutz-Grundverordnung (DSGVO) oder der GoBD.

Vorschlag für die Vorgehensweise in Immobilienfirmen

4. **Schulung von Mitarbeitenden**: Alle Mitarbeitenden sollten in den Grundsätzen des Datenschutzes und der DSGVO geschult werden, um sicherzustellen, dass sie die Verarbeitung personenbezogener Daten verstehen und sich an die geltenden Bestimmungen halten.

Empfehlungen zur Schulung von Mitarbeitenden zu DSGVO und TOM

1. **Regelmäßige Schulungen**: Die Schulungen sollten regelmäßig stattfinden, damit die Mitarbeitenden auf dem aktuellen Stand bleiben und Änderungen oder Anpassungen in den TOM schnell umsetzen können.
2. **Schulungsthemen**: Sowohl die rechtlichen Anforderungen der DSGVO, als auch technische Themen des Datenschutzes und der IT-Sicherheit sowie Cybersichrheit sind aktuelle Schulungsthemen, die umgesetzt werden sollen.
3. **Praxisnahe Schulungen**: Die Schulungen sollten praxisnah gestaltet sein und konkrete Beispiele aus dem Arbeitsalltag enthalten, damit die Mitarbeitenden die TOM besser verstehen und im Arbeitsalltag umsetzen können.
4. **Zielgruppenspezifische Schulungen**: unterschiedliche Bedürfnisse und Anforderungen der Mitarbeitenden, z.B. Schulung für IT-Abteilung anders gestaltet sein als die Schulung für die kaufmännischen Mitarbeiter.
5. **Dokumentation**: Die Schulungen sollten dokumentiert werden, damit nachvollzogen werden kann, welche Mitarbeiter welche Schulung besucht haben und welche Inhalte vermittelt wurden.
6. **Sensibilisierung**: Die Schulungen sollten nicht nur auf die TOM fokussieren, sondern auch auf die Sensibilisierung der Mitarbeitenden im Umgang mit personenbezogenen Daten. Dabei sollten auch Risiken und Gefahren aufgezeigt werden, damit die Mitarbeitenden ein Bewusstsein dafür entwickeln, wie wichtig der Datenschutz ist.
7. **Schulungsformate**: Es sollten verschiedene Schulungsformate angeboten werden, wie z.B. Präsenzschulungen, E-Learning oder Webinare. So können die Schulungen flexibler gestaltet werden und auf die Bedürfnisse der Mitarbeitenden eingegangen werden.
8. **Kontrolle**: Die Wirksamkeit der Schulungen sollte regelmäßig überprüft werden, z.B. durch Tests oder Prüfungen. So kann sichergestellt werden, dass die Mitarbeitenden die TOM verstanden haben und im Arbeitsalltag umsetzen können.

Wir freuen uns auf ein Wiedersehen/-hören auf einer der Veranstaltungen / Webinare oder als
Anwender der Datenschutz-Police – unsere nächsten Termine:

07. und 08.05.2024 – digiKon 9.0 -> www.digikonreal.de

Sprechen Sie uns gern an und buchen unter office@datenschutz.immobilien

Weitere Informationen und Buchung

unter www.datenschutz.immobilien

office@datenschutz.immobilien