Kundeninformation
"Datenpanne und die DSGVO"

id newmedia KnowHow - für *Sie ...*

40 Jahre Erfahrung, 40 Jahre Dienst am Kunden

- ganzheitliche, sichere IT-Lösungen auch für kleinste Unternehmen
- ganzheitliche, sichere IT-Lösungen für Behörden
- DSGVO / BDSG-neu Umsetzung
- Analyse kritischer IT-Sicherheitsstrukturen
- Digitales Klassenzimmer in Schulen
- Digitales Büro
- Computer Forensik

id newmedia Einsteinstrasse 24 82152 Planegg-Martinsried 0160-48 28 918
id newmedia Büro Germering 089-899 799 39 info@id-newmedia.de www.id-newmedia.de USt.-Id Nr. DE128145303

Bild : animationfactory

Ein Sachbearbeiter veröffentlichte aus Versehen Daten ? Ein Dieb hat Ihren Laptop oder einen USB-Stick gestohlen ? Hacker haben Ihr Unternehmen angegriffen ? Sicherheitsverstöße sind nicht gerade selten und der Alptraum eines jeden seriösen Unternehmens. Sollte auch Ihr Unternehmen betroffen sein, so handeln Sie sofort und schnell !

 im Februar 2021

Die DSGVO schreibt nämlich vor, Datenpannen umgehend zu melden.

DSGVO : Datenpanne – was ist das ?
DSGVO : Datenpanne - und Risiko ?
DSGVO : Datenpanne melden – Zeitfenster ?
DSGVO : Datenpanne – was ist anzugeben ?
DSGVO : Datenpanne – keine Meldung … keine Strafe ?
DSGVO : Datenpanne – Auftragsverarbeiter, was ist zu tun ?

DSGVO : Datenpanne – was ist das ?

Ihr Unternehmen ist von einer Datenschutzverletzung betroffen ? Dann müssen Ihr Unternehmen jetzt aus Gründen der Datensicherheit prüfen, ob es sich um eine Datenpanne handelt. Ihr Unternehmen sind nicht dazu verpflichtet, bei jedem Datenleck eine Meldung der Datenpanne bei der Aufsichtsbehörde einzureichen. Ihr Unternehmen muß eine Datenpanne nur melden, wenn diese für den Betroffenen nach dem Stand der Ermittlung mit Risiken verbunden ist.

Eine Verletzung personenbezogener Daten liegt nach Art. 4 Nr. 12 DSGVO immer dann vor, wenn personenbezogene Daten verlorengegangen sind, vernichtet, verändert oder unbefugt offengelegt wurden.

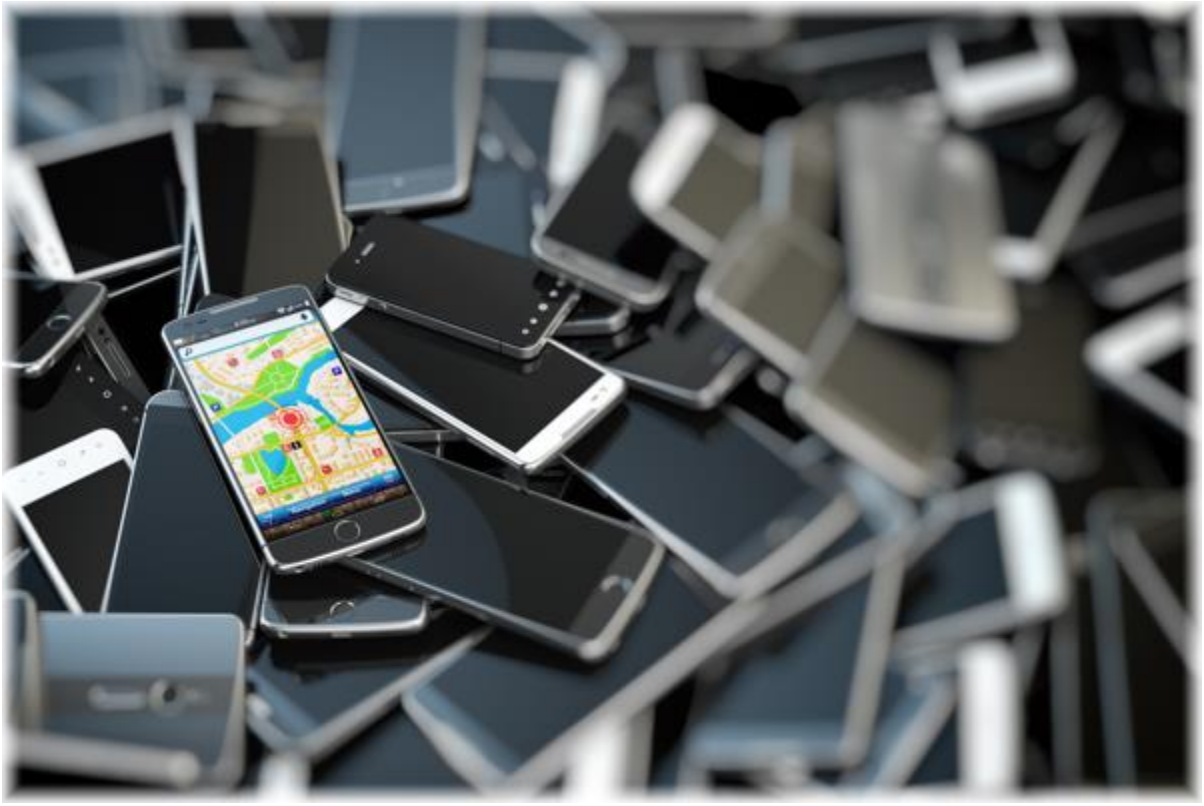

Bild : animationfactory

<u>Beispiel</u>

Ein Mitarbeiter verliert einen Laptop oder ein Mobiltelefon mit personenbezogenen Daten oder Hacker greifen Ihre Datenbank an und stehlen personenbezogene Daten oder Diebe brechen ein und stehlen Dokumente oder ziehen Daten auf einen USB-Stick. Auch eigene unzufriedene Mitarbeiter sind ein Risikofaktor.

Datenpanne durch Social Engineering

Social Engineering (auch „soziale Manipulation“) nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen oder personenbezogenen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.

Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Informationen oder unbezahlte Dienstleistungen zu erlangen.

Häufig dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche oder personenbezogene Daten einzusehen; man spricht dann auch von Social Hacking.

Das Grundmuster des Social Engineering zeigt sich bei fingierten Telefonanrufen : der Social Engineer ruft Mitarbeiter eines Unternehmens an und gibt sich als Techniker aus, der vertrauliche Zugangsdaten benötigt, um wichtige Arbeiten abzuschließen.

Bereits im Vorfeld hat er aus öffentlich zugänglichen Quellen oder vorangegangenen Telefonaten kleine Informationsfetzen über Verfahrensweisen, tägliches Bürogerede und Unternehmenshierarchie zusammengetragen, die ihm bei der zwischenmenschlichen Manipulation helfen, sich als Insider des Unternehmens auszugeben.

Zusätzlich verwirrt er sein technisch ungebildetes Opfer mit Fachjargon, baut mit Smalltalk über scheinbar gemeinsame Kollegen Sympathie auf und nutzt Autoritätsrespekt aus, indem er droht, bei vom Opfer unterlassener Kooperation dessen Vorgesetzten stören zu müssen.

Unter Umständen hat der Social Engineer bereits im Vorfeld Informationen gesammelt, dass ein bestimmter Mitarbeiter sogar wirklich technische Hilfe angefordert hat und bereits tatsächlich einen derartigen Anruf erwartet.

Trotz ihrer scheinbaren Banalität gelingen mit der Methode immer wieder spektakuläre Datendiebstähle, unter denen sich in der Regel auch personenbezogene Daten befinden.

Ist die Identität des Absenders einer email nicht sicher, sollte man stets mißtrauisch sein.
Bei Anrufen sollten auch scheinbar unwichtige Daten nicht sorglos an Unbekannte weitergegeben werden, da diese die so erhaltenen Informationen für weitere Angriffe nutzen können.

Bei Antworten auf eine E-Mail-Anfrage sollten unter keinen Umständen persönliche oder finanzielle Daten preisgegeben werden, egal von wem die Nachricht zu kommen scheint.
Keine Links aus emails verwenden, die persönliche Daten als Eingabe verlangen. Statt dessen die URL selbst im Browser eingeben.

Bei Unklarheit über die Echtheit des Absenders diesen nochmals telefonisch kontaktieren, um die Authentizität der email zu überprüfen.

Sie sind Datenverarbeiter ? Eine Hausverwaltung ? Ein Steuerberater ?

Als Datenverarbeiter jegliche Couleur unterliegen Ihr Unternehmen einer Dokumentationspflicht. Dokumentieren Sie und Ihr Unternehmen den Vorfall sofort und bewerten Sie und Ihr Unternehmen in einer nachgelagerten Risiko-Analyse, ob Ihr Unternehmen die Datenpannen melden muß oder nicht.

Bild : animationfactory

DSGVO : Datenpanne - und Risiko ?

Ihr Unternehmen haben einen Rechner oder Kopierer entsorgt, haben aber die Daten nicht vom internen Speicher (HDD, SSD …) gelöscht ? Bei verschlüsselten Daten sind Folgeschäden weniger wahrscheinlich.

In solch einer Situation besteht wohl keine Meldepflicht nach der DSGVO. Denken Ihr Unternehmen aber daran, daß Ihr Unternehmen bei einer meldepflichtigen Datenpanne sowohl die Behörde als auch die Betroffenen informieren müssen.

Apropos Aufsichtsbehörde : die Meldepflicht besteht schon bei einem „normalen Risiko“.

Apropos Betroffene : Betroffene sind erst dann zu benachrichtigen, wenn die Schutzverletzung ein „gesteigertes Risiko“ für ihre Rechte und Freiheiten auslöst.

<u>Beispiel</u>

Entsorgt Ihr Unternehmen eine funktionierende Festplatte, ist es möglich, daß diese aus dem Müllbehälter entnommen wird (es könnte sich auch um Betriebsspionage handeln).

Bei einer verschlüsselten Festplatte sind die Daten aber nur unter einem erheblichen Aufwand oder gar nicht zu entschlüsseln. Das Risiko, daß Schädiger die Sicherheitslücke ausnutzen, ist also sehr gering.

Ihr Unternehmen ist in einer solchen Situation trotzdem eventuell verpflichtet, den Vorfall der Aufsichtsbehörde zu melden.

Bild : animationfactory

Da das Risiko aber nicht „gesteigert“ ist, entfällt zumindest die Meldepflicht gegenüber den Betroffenen – also gegenüber denjenigen Personen oder Geschäftspartnern / Kunden, deren personenbezogene Daten auf der Festplatte gespeichert sind.

In den folgenden Situationen besteht nach Art. 34 III DSGVO bzw. § 42a BDSG–alt keine Meldepflicht :

- Ihr Unternehmen traf technische und organisatorische Sicherheitsvorkehrungen (z.B. Verschlüsselung) und hat diese dokumentiert (Verarbeitungsverzeichnis).

- Ihr Unternehmen stellt durch nachgelagerte Maßnahmen sicher, daß höchstwahrscheinlich kein Risiko mehr besteht;

- die Meldung betrifft einen großen Personenkreis, der nur schwer zu ermitteln ist. Dann muß Ihr Unternehmen jedoch auf andere Maßnahmen ausweichen, z. B. sogar auf eine öffentliche Bekanntmachung. Ob eine Meldepflicht besteht oder nicht, hängt also immer von der jeweiligen Situation ab.

DSGVO : Datenpanne melden – Zeitfenster ?

Bild : animationfactory

Liegt eine Datenpanne vor, muß Ihr Unternehmen diese der zuständigen Datenschutzbehörde innerhalb von 72 Stunden anzeigen.

Bei der betroffenen Person bzw. dem betroffenen Unternehmen gelten andere zeitliche Vorgaben. Hier ist Ihr Unternehmen dazu verpflichtet, die Meldung unverzüglich durchzuführen.

„Unverzüglich“ bedeutet, daß Ihr Unternehmen die Meldung so schnell wie nur möglich durchführen – ohne nachweisbar schuldhafte Verzögerung.

Regel

Je risikobehafteter die Datenschutzverletzung ist, desto schneller sollte die Meldung erfolgen.

In dem Beispiel mit der Festplatte reicht eine Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden aus. Das Datenleck ist den Betroffenen nicht zu melden, da es unwahrscheinlich ist, daß jemand die Daten entschlüsselt. Sollten Ihr Unternehmen dennoch einer Meldepflicht unterliegen, können Sie sich ausreichend Zeit lassen. Denn es ist unwahrscheinlich, daß ein Schädiger die Festplatte aus dem Müll heraussucht.

Sollte dies dennoch geschehen, müßte er zunächst die Verschlüsselung umgehen, was viel Zeit beansprucht – und sich in der Regel nicht für ihn rechnet.

Ob eine Datenpanne also zu melden ist, hängt davon ab, ob ein Risiko für die Rechte und Freiheiten der betroffenen Person oder Ihres Kunden vorliegt und wie dieses zu bewerten ist.

Deshalb sollte Ihr Unternehmen Datenschutzverstöße immer zumindest intern dokumentieren.

In einer anschließenden Risiko-Analyse ist dann zu klären, ob tatsächlich ein Risiko vorliegt und ob das Datenleck der Aufsichtsbehörde oder auch den Betroffenen zu melden ist.

DSGVO : Datenpanne – was ist anzugeben ?

Zunächst sollte Ihr Unternehmen eine Meldung erstellen. Der Umfang dieser Meldung hängt davon ab, ob Ihr Unternehmen nur an die Aufsichtsbehörde oder auch an einen Betroffenen erfolgt.

Meldung gegenüber der Aufsichtsbehörde

Die Meldung gegenüber der Aufsichtsbehörde richtet sich nach Art. 33 DSGVO. Meldungen müssen die folgenden Punkte enthalten :

- welche Art von Verletzung liegt vor (Datenverlust, Diebstahl usw.) ?
- wer sind die Betroffenen (Kunden, Mitarbeiter, Geschäftspartner) ?
- wie viele Betroffene gibt es ?
- welche Art von Datensätzen ist betroffen ?
- Name und Anschrift des Datenschutzbeauftragten ?
- welche Folgen zieht die Schutzverletzung nach sich (z.B. finanzielle Nachteile) ?
- welche Schutzmaßnahmen hatte Ihr Unternehmen ergriffen / möchte Ihr Unternehmen ergreifen ?
- welche Gegenmaßnahmen sind noch denkbar ?

Das Gesetz schreibt nicht vor, daß die Meldung per email oder Brief eingereicht werden muß. Es ist zu empfehlen dies aber schon aus Beweisgründen zusätzlich zu tun. Trotzdem – schon aus Grund der Frist - sollte Ihr Unternehmen die zuständige Aufsichtsbehörde zuerst telefonisch kontaktieren und dies dokumentieren.

Denken Sie daran, daß Ihr Unternehmen der Datenschutzbehörde den Verstoß innerhalb von 72 Stunden melden muß. Wenn Ihr Unternehmen die telefonische Meldung nicht durchführt, riskiert Ihr Unternehmen ein Bußgeld.

Meldung gegenüber den Betroffenen

Ihr Unternehmen möchte eine Meldung an die Person oder den Geschäftspartner senden, die von dem Datenleck betroffen sind ? Ihr Unternehmen muß den Betroffenen keine umfassenden Informationen über die Datenschutzverletzung bereitstellen, aber die folgenden Informationen muß Ihr Unternehmen auf jeden Fall der zuständigen Datenschutzbehörde übermitteln :

- Name und Anschrift des Datenschutzbeauftragten
- Art der Schutzverletzung
- wahrscheinliche Folgen der Datenschutzverletzung
- ergriffene und empfehlenswerte Gegenmaßnahmen

Frage : wie machen Sie das eigentlich ohne Verarbeitungsverzeichnis ?

Für Ihr Unternehmen ist die Aufsichtsbehörde des Bundeslandes zuständig, in dem Ihr Unternehmen seinen Sitz hat. Es kommt ausschließlich darauf an, wo der Sitz des Unternehmens ist; wo sich die handelnde Zweigstelle, Filiale oder Geschäftsstelle befindet, ist irrelevant.

DSGVO : Datenpanne – (k)eine Meldung … (k)eine Strafe ?
Die Datenschutzbehörden haben ein Ermessen, dürfen also unter mehreren Optionen wie z. B. einer Verwarnung und einer Geldbuße im Einzelfall auswählen.

Welche Option die Datenschutzbehörden auswählen **wenn die Datenpanne doch herauskommt** hängt immer von der individuellen Situation und dem Verhalten der Gegenseite – also Ihnen - ab.

Die DSGVO stellt die Nichterfüllung von Meldepflichten unter Strafe, Art. 83 IVa DSGVO. Es sind Bußgelder in Höhe von bis zu zehn Millionen Euro möglich, oder bis zu zwei Prozent des weltweiten Umsatzes des vorherigen Geschäftsjahrs. Die Datenschutzbehörden setzen diese Strafen auch tatsächlich durch. Dies bewiesen Beispiele der jüngeren Vergangenheit.

DSGVO : Datenpanne – Auftragsverarbeiter, was ist zu tun ?
Es liegt eine Datenpanne bei einem Auftragsverarbeiter vor ? Auftragsverarbeiter unterliegen keiner Meldepflicht. Ihr Unternehmen ist aber dazu verpflichtet, denjenigen zu unterstützen, der meldepflichtig ist. Die DSGVO schreibt dem Auftragsverarbeiter in Art. 28 DSGVO nicht genau vor, was er zu machen hat. Nehmen Sie und Ihr Unternehmen deshalb schon beim Vertrag zur Auftragsverarbeitung entsprechende Regelungen auf. Diese können sich auf Umfang der Unterstützungspflicht, bereitzustellende Informationen und damit verbundene Fristen beziehen.

Beachten Sie immer, daß Ihr Unternehmen einer Dokumentationspflicht gem. Art. 33 Abs. 5 DSGVO unterliegt.

(1) Erstellen Sie oder lassen Sie einen Ablaufplan erstellen;

(2) Erstellen Sie (oder lassen Sie erstellen) einen Tätigkeitsbericht für die interne Aufbereitung;

(3) Beurteilen Sie, wie bereits erwähnt, ob Ihr Unternehmen einer Meldepflicht unterliegt.

(4) Kontaktieren Sie im Problemfall die zuständige Datenschutzbehörde vorab telefonisch.

(5) Lassen Ihr Unternehmen bereits im Vorfeld von Datenschutzexperten beraten,

Stichwort : Risiko-Analyse !

(6) Schulen Sie Ihre Mitarbeiter im Umgang mit einem Datenverlust.

Wir beraten Sie gerne …