Verlag für
Neue Medien
DATA COMMUNICATIONS GMBH

IT-Sicherheits- und Datenschutzkonzept mit technischen und organisatorischen Maßnahmen

Stand 22. Mai 2018

Gültigkeit

Verlag für Neue Medien GmbH, Bötzinger Str. 48, 79111 Freiburg, www.vfnm.de
ecomuc gmbh, Freiburger Str. 33, 79427 Eschbach, www.ecomuc.de

Ziel des IT-Sicherheits- und Datenschutzkonzeptes

Das Datenschutzkonzept dient der Dokumentation und ist Basis für Kontrollen der Sicherheit für Daten im Interesse eines geregelten und sicheren Geschäftsablaufs, der Einhaltung der berechtigten Schutzbedürfnisse von Personen bzgl. ihrer persönlichen Daten. Es dient dem Schutz des Unternehmens und seiner Kommunikationsinfrastruktur und dient damit der langfristigen Sicherung der Existenz unseres Unternehmens. Es hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen z. B. durch Auftraggeber im Rahmen der Auftragsverarbeitung genutzt werden. Dadurch soll nicht nur die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) gewährleistet werden, sondern auch der Nachweis der Einhaltung vieler Maßnahmen für einen professionellen, zuverlässigen, fairen und partnerschaftlichen Geschäftsablauf geschaffen werden.

Präambel

Der Verlag für Neue Medien Data Communications GmbH wirkt seit 1995 aktiv am Aufbau und der Erschließung des Nutzens des Internets und dessen Möglichkeiten für Unternehmen und Privatpersonen mit. Die Kommunikation im Internet ist eine moderne, nützliche und einfache Art der zwischenmenschlichen Kommunikation. Es gehört zum guten Ton, sich beim Gespräch gegenseitig mit Namen vorzustellen. Und es wird als angenehm empfunden, wenn sich Menschen bei der nächsten Begegnung noch an einen erinnern. Und mancher freut sich sogar über einen Glückwunsch zum Geburtstag. Insofern erscheinen Regelungen der DSGVO zumindest teilweise fraglich, wenngleich der Grundgedanke richtig und wichtig ist.

Dem Datenschutz und dem fairen Umgang mit persönlichen oder betrieblichen Daten von Geschäftspartnern trägt der Verlag für Neue Medien Data Communications GmbH aus Überzeugung schon seit Beginn seiner Tätigkeit auch in Bereichen außerhalb des Internets nach bestem Können, Wissen und Gewissen Rechnung.

Datenschutzpolitik und Verantwortlichkeiten im Unternehmen

Der Verlag für Neue Medien GmbH ist ein Kommunikationsunternehmen, dessen Arbeitsabläufe und Kommunikation in Großraumbüros stattfindet. Insofern sind alle Mitarbeiter an Kommunikation aktiv oder passiv beteiligt und deswegen grundsätzlich in firmeninternen Regelungen zur Geheimhaltung verpflichtet. Als Anbieter von Serviceleistungen im Internet müssen alle Arbeitsplätze grundsätzlich Kommunikationsaufgaben im Internet wahrnehmen können und die produktiven IT-Systeme sind permanent weltweiten Angriffen (Datenzugriff,

Datenänderung, Datenlöschung, Datenverschlüsselung) ausgesetzt. Alle Systeme sind deswegen auf einem hohen Niveau gesichert und jeweils nach dem aktuellen Stand der Technik geschützt, soweit dies finanziell und organisatorisch möglich ist. Mitarbeiter kennen die ständigen Gefahren und sind entsprechend aufmerksam und vorsichtig.

Als kleines Unternehmen ist es nur möglich eine zeitliche Verfügbarkeit der Serviceleistung für Kunden zu bieten, wenn der Service nicht personengebunden ist. Deshalb können in der Regel alle oder viele Serviceleistungen erbringen und haben zur Gewährleistung schneller Reaktionen (z.B. Abwehr von Angriffssituationen) dem jeweiligen Know-how angemessen weitgehende Rechte auch zur Administration. Im Rahmen einer fundierten Ausbildung erhalten z.B. auch Auszubildende früh Zugang zu personenbezogenen Daten und Systemen der Datensicherung und Administration.

Aus eigenem Interesse und zur Sicherstellung eines hohen Niveaus der Services
für Kunden lebt der Verlag für Neue Medien GmbH eine kontinuierliche Sicherstellung und bei Bedarf eine Verbesserung seines Datenschutzmanagementsystems.

Im Interesse einer hohen Verfügbarkeit der Dienstleistung erfolgt ständig auch durch ständige Beobachtung der Geschehnisse und Erfordernisse im Internet und dem Wissensaustausch im Team eine Schulung, Sensibilisierung und Verpflichtung der Mitarbeiter.

Rechtliche Rahmenbedingungen im Unternehmen

Als Anbieter im weltweiten Internet mit internationalem Anschuss und internationaler Kommunikation zwischen Besuchern und Anbietern bzw. Kunden und Interessenten ist es unmöglich alle gesetzlichen Regelungen zu kennen. Im Grundsatz ist die seit 25 Jahren entwickelte Unternehmenskultur und die Grundideen und die Unternehmensphilosophie eine sichere Grundlage, dass der Umgang mit personenbezogenen Daten in der Regel die meisten und vor allem die sinnvollen rechtlichen Regeln – durchaus auch weltweit – einhält.

Alle Geschäftspartner des Verlags für Neue Medien
bewegen sich im Internet und haben ein gemeinsames Interesse an einem sicheren, reibungslosen, schnellen und fairen Kommunikationsablauf und einem partenerschaftlichen Umgang bei der Lösung eventuell auftretenden Probleme.

Alle anwendbaren Gesetze mit ggf. lokalen Sonderregelungen
kann ein sehr kleines und hoch leistungsfähiges Unternehmen mit weltweiter Geschäftstätigkeit, dessen Geschäft ausdrücklich nicht die oft auf komplizierte Gesetzesformulierungen und auf sich gerne auch einmal widersprechende Grundsatzurteile basierende Rechtinterpretation oder Rechtsauslegung ist, nicht kennen. Sofern Gesetze und Regelungen dem gesunden Menschenverstand entsprechen, einen friedlichen, freiheitlichen, gleichberechtigten, demokratischen, sinnvollen und machbaren Ansatz verfolgen und etwas grundsätzlich möglich machen wollen und nicht verhindern wollen, genügt dem Verlag für Neue Medien der gesunde Menschenverstand und der Spaß daran, etwas aufzubauen und zu bewegen. Wenngleich durchaus auch die oft als vorbildlich beschriebene deutsche Politik und Entscheidungen deutscher Gerichte in Einzelfällen schon bewiesen haben, dass unser gesunder Menschenverstand z.B. in Deutschland nicht immer ausreicht.

Dokumentation

Schutzbedarf der Daten unter Berücksichtigung von Machbarkeit und Sinnhaftigkeit Für alle internen personalbezogenen Daten hoch, für Kundenaufträge und in internen Internetbereichen verfügbar gemachte Daten mittel und für alle im Internet ohne Zugangsschutz bereitgestellten Daten (z.B. Homepages, Kundeneinträge auf Plattformen) niedrig.

Durchgeführte interne und externe Überprüfungen
Alle betreuten Systeme werden ständig oder je nach Bedarf in regelmäßigen Abständen beobachtet und obliegen z.B. bei Bearbeitungstätigkeiten der automatisch der Kontrolle aller Beteiligten. Öffentlich zugängliche Daten sind z.B. in Suchmaschinen indiziert und für jeden auffindbar und auf Richtigkeit prüfbar. Unerwünschte oder unrichtige Daten werden in der Regel wegen des hohen Qualitätsanspruchs an die gespeicherten und bereitgestellten Daten mit hoher Priorität korrigiert.

Bestehende technische und organisatorische Maßnahmen (TOM)

Ziele, Philosophie und Grundsätze
Geeignete technische und organisatorische Maßnahmen, die unter Berücksichtigung u. a. des Zwecks der Verarbeitung, des Stands der Technik und der Implementierungskosten sinnvoll zu treffen und nachzuweisen sind.

Betroffenenrechte
Grundsätzlich werden nur Daten gespeichert und verarbeitet, die Betroffene zu diesem Zweck bereitgestellt haben. Sofern keine Vorgaben für steuerliche oder rechtliche Dinge bekannt sind, befürchtet oder auch nur vermutet werden, wird mit diesen Daten bzgl. Löschung, Änderung, Weitegabe auf Anfrage bzw. Weisung des Bereitstellers verfahren.

Zugangssteuerung
Dient vor allem der Sicherstellung, dass Daten nicht unbeabsichtigt veröffentlicht, übertragen, verändert oder gelöscht werden. Deshalb sichern Zugriffskonzepte weitgehen, dass nur Mitarbeiter Zugriff auf Daten haben, die zielführend und nutzenbildend damit umgehen können.

Informationsklassifizierung
Es gibt vier Stufen der Berechtigungen im Netzwerk: „Admins“ haben Vollzugriff, Mitglieder „Verwaltung“ haben Zugriff auf Personal und Buchhaltung, Mitglieder „Web“ haben Zugriff auf Daten von Kundenprojekten und Mitglieder „Temp“ haben Zugriff auf freie Datenbereiche oder temporäre Kopien (z.B. Praktikanten). Darüber hinaus gibt es auch ausschließlich lokale Berechtigungen auf einzelnen Rechnern (z.B. nur Internetzugriff).

Physische und umgebungsbezogene Sicherheit
Die Verarbeitung findet an zwei mit VPN verbundenen Standorten statt. Deswegen sind interne Dateibereiche immer doppelt vorhanden (Replikation in der Regel werktäglich), wobei jeweils nur eine Seite schreiben kann. Dadurch ist z.B. eine umfängliche „versehentliche“ oder von außen böswillig initiierte Verschlüsselung weitgehend unmöglich.

Datenverarbeitung auf Endgeräten
Erfolgt nur nach Anmeldung und Benutzeridentifikation. Endgeräte stehen im Geschäftsbetrieb unter Beobachtung aller anwesenden Mitarbeiter. Jeder Mitarbeiter ist für die Sicherheit seines Arbeitsplatzes verantwortlich, was eine Abmeldung und das Ausschalten nach Dienstschluss angeht. Alle Geräte werden zentral mit aktueller Virenschutzsoftware versorgt, sind durch Firewall geschützt und haben aktuelle Systemsoftwareversionen.

Datensicherung
Erfolgt für Daten auf Servern zentral auf Sicherungssysteme auch standortübergreifend. Darüber hinaus hat jeder Anwender eine persönliche Verantwortung, seine Datenbestände zusätzlich auf seinen Arbeitsplatz und /oder externe Datenträger (z.B. Sticks)zu sichern.

Informationsübertragung
Per VPN-Netzwerk verschlüsselt zwischen den Standorten. Zu internen und externen Internet-Servern (z.B. bei Housing-/Hostingpartnern) per SSL-VPN und/oder über IP-Bereiche geschränkt.

Schutz vor Schadsoftware
Durch aktuelle Systeme, Firewalls mit Virenschutz und Spamschutz. Außerdem interne Kommunikation über aktuelle Gefahrenlagen. Einige Email-Konten werden bevorzugt auf alphanumerischen Email-Programmen bearbeitet und Email-Anhänge nur von bekannten Absendern (u.U. nach Header-Kontrolle) geöffnet.

Handhabung technischer Schwachstellen
Der Verlag verfügt über jahrzehntelange Routine bei der Abwehr von Angriffen aus der Internet und berät auch Kunden. In der Regel wird eine außergewöhnliche hohe Verfügbarkeit und Sicherheit erreicht. Ausfälle verursachten bisher in den meisten Fällen sogar die eigentlich zur besseren Verfügbarkeit eingesetzten Sicherheitssysteme (z.B. USV-Anlagen).

Kryptografische Maßnahmen
Werden vor allem für die Verschlüsselung von Passwörtern eingesetzt.

Kommunikationssicherheit
Obwohl eigentlich nicht wichtig, weil für Späher uninteressant, für z.B. Anfrageformulare realisiert. Eingehende verschlüsselte Dokumente werden in der Regel aus Sicherheitsgründen sofort gelöscht. Passwortgeschützte PDFs behindern mehr als sie nutzen.

Privatsphäre und Schutz von personenbezogenen Informationen
Wir sind wenige und wissen voneinander mehr als wir abgespeichert haben. Und die Daten von anderen wollen wir nur in dem Umfang haben, damit wir für sie tätig werden können. Weil wir aber schon neugierige Mitarbeiter hatten, haben wir bzw. zuständige Mitarbeiter für aus unserer Sicht sensible Daten Zusatz-Maßnahmen getroffen.

Lieferanten Beziehungen
Wir suchen nur Lieferanten, die besser sind und mehr können als wir selbst. Das überprüfen wir ständig, weil von einer guten Zusammenarbeit das gemeinsame Ergebnis, die hochqualitative Leistung für unsere Kunden und Geschäftspartner abhängt und weil wir Geld dafür bezahlen. Maß sind hier nicht politische Vorgaben mit Verpflichtungen zu Verträgen, die am Ende Unterlassungserklärungen gleichkommen, sondern unser eigener hoher und realistischer Anspruch.