Digitalisierung

Das Schlagwort „Digitalisierung" ist wieder einmal in aller Munde. Unternehmen und die öffentliche Verwaltung lagern die Arbeit großenteils ins „Home-Office" aus und sogar der Schulunterricht wird übergangsweise ebenfalls zum „Home-Schooling" umfunktioniert. Für all dies ist eine Digitalisierung der zu Grunde liegenden Prozesse eine unabdingbare Voraussetzung.

Viele öffentliche Einrichtungen, aber auch zahlreiche kleine und große Unternehmen mussten dabei feststellen, dass längst nicht alle Geschäftsprozesse angemessen darauf vorbereitet waren. Die Probleme sind vielfältig: von fehlender Hardware- und Softwareausstattung für das Home-Office, über fehlende Kompetenzen der Beteiligten, die Prozesse nunmehr „virtuell" abzubilden, bis hin zu umfangreichen Vorgaben bzgl. Datenschutz und Informationssicherheit.

Dabei hat Digitalisierung eine funktionale und eine rechtliche Facette. Zu ersterer gehört die Informationssicherheit und rechtlich ist es der Datenschutz, dessen vielschichtiger Vorgabenkatalog sich nur selten vollständig umsetzen lässt. Die Berücksichtigung dieser Aspekte darf aber nicht zum „Totschlagsargument" werden, es sind pragmatische Vorgaben gefragt, die bzgl. ihrer Nutzbarkeit auch den „Praxistest" bestehen.

Die einzelnen Beiträge im Überblick

Der Schwerpunkt „Datenschutz und -sicherheit in der öffentlichen Verwaltung" widmet sich den Herausforderungen aus unterschiedlichen Blickwinkeln:

- Der Beitrag **„Cyber-Security: Ein Fundament für die Digitalisierung von Staat und Verwaltung"** von Dominik Kammerloher beleuchtet die Relevanz der Informationssicherheit für die Digitalisierung.
- Ernst-Günther Giessmann, Franziska Granc und Arno Fiedler stellen im Beitrag **„Rechtskonforme Prüfung elektronischer Signaturen gestern und heute"** die Entwicklung der elektronischen Signatur sowie die Prüfung derselben dar und geben einen Ausblick auf die Herausforderungen bei „Smart Contracts".
- Kai Martius stellt im Beitrag **„SINA: Sicherheit als Infrastruktur betrachtet"** die „Sichere Inter-Netzwerk Architektur (SINA)" vor und zeigt auf, wie diese zur Kommunikationssicherheit beitragen kann.
- Marit Hansen und Thomas Probst beschreiben im Beitrag **„Die ambivalente Beziehung zwischen eGovernment und Datenschutz"** das Spannungsverhältnis des Datenschutzes als Hemmschuh und als Grundlage für eine erfolgreiche Digitalisierung.
- Im Beitrag **„Business Continuity im Föderalismus"** zeigt Thomas Milde dann die Möglichkeiten und Herausforderungen bei der Absicherung der ITK-Netze der öffentlichen Verwaltung auf.
- Dominik Birk thematisiert im Beitrag **„Managed Security Services: Hilfe oder Herausforderung für die Informationssicherheit?"** die Auslagerung von sicherheitsrelevanten Diensten und hinterfragt die Vor- und Nachteile.
- Joerg Heidrich und ich selbst diskutieren im Beitrag **„Dauerhaft sicher zu Hause: Datenschutz und Informationssicherheit im Home-Office"** bestehende Vorgaben und Hilfestellungen und ob diese realistisch umsetzbar sind.

Ergänzt wird dieser Schwerpunkt durch zwei weitere Beiträge: Der Aufsatz **„Was informatisch richtig ist, kann auch juristisch recht sein"** von Kai von Lewinski und Johanna Hähnle diskutiert die Frage, ob und wie sich die technischen Begriffe „Datenqualität" und „Datenvalidität" in den rechtlichen Kontext übertragen lassen. Eberhard von Faber regt im Forum mit dem Beitrag **„Zur Zukunft des IT-Sicherheitsmanagements angesichts des Wandels von Technik und Serviceerbringung"** schließlich eine offene Diskussion über die zukünftige Ausprägung des IT-Sicherheitsmanagements an.

Wir haben uns mit den vorliegenden Beiträgen wie immer um eine interessante Auswahl bemüht und hoffen, dass sie Ihnen viele Anregungen für Ihre eigenen Projekte geben. Zusammen mit dem gesamten Herausgeberteam wünsche ich Ihnen als Gastherausgeber eine spannende Lektüre. Und bitte bleiben Sie gesund!

Christoph Wegener