ist: In § 191a GVG ist künftig vorgesehen, dass die Übermittlungswege und elektronische Dokumente im elektronischen Rechtsverkehr barrierefrei zu gestalten sind. Gleiches gilt für elektronische Formulare und die Ausgestaltung des besonderen Postfachs der Rechtsanwälte und des Schutzschriftenregisters.

7. Zeitplan für das Inkrafttreten

Die in dem Gesetzentwurf vorgesehenen Maßnahmen sollen schrittweise in Kraft treten. Schon am Tag nach der Verkündung tritt die Vorschrift über den Beweiswert von Scannprodukten in Kraft, damit auf diesem Gebiet Rechtssicherheit eintritt. Am 1. Juli 2014 sollen die Beweisvorschrift für De-Mail-Nachrichten sowie die Vorschriften Gültigkeit erlangen, die eine Zustellung von Urteilen und Beschlüssen nicht mehr in Ausfertigung, sondern nur noch in beglaubigter Abschrift vorsehen. Zum 1. Januar 2016 sollen die Vorschriften über das Schutzschriftenregister sowie über das elektronische Anwaltspostfach in Kraft treten.

Ab 1. Januar 2018 soll der elektronische Zugang zu allen deutschen Gerichten ohne qualifizierte elektronische Signatur bei Nutzung eines sicheren Übermittlungsweges eröffnet sein. Da einzelne Länder für die Einrichtung der notwendigen IT-Infrastruktur mehr Zeit benötigen, erlaubt der Entwurf, das Inkrafttreten der Zugangsregelungen durch Länderverordnung bis zum 1. Januar 2020 hinauszuschieben. Spätestens ab diesem Zeitpunkt ist der elektronische Zugang zu den Gerichten bundeseinheitlich eingeführt. Eine Pflicht zur Nutzung des elektronischen Rechtsverkehrs für Rechtsanwälte und Behörden können die Länder frühestens ab 2020 vorsehen, wobei eine einjährige Phase der Freiwilligkeit im betreffenden Land vorauszugehen hat. Bundesweit tritt die Nutzungspflicht 2022 in Kraft.

Den Gesetzentwurf in der vom Bundesrat angenommenen Fassung finden Sie hier: *http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/Elektron.Rechtsverkehr.html?nn=1468684*

EU-Agentur für Cybersicherheit ENISA erhält weitere Aufgaben

Die Europäische Agentur für Netz-und Informationssicherheit, ENISA, hat am 18 Juni 2013 eine neue Verordnung erhalten, die ihr ein Mandat über sieben Jahre mit einem erweiterten Spektrum an Aufgaben gewährt. Die Verordnung wurde in der Ausgabe des Amtsblatts der Europäischen Union veröffentlicht [*http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF*] und ist am 19 Juni 2013 in Kraft getereten.

Die ENISA-Verordnung wurde vom Rat der Europäischen Union am 14. Mai 2013 gebilligt, nachdem sie durch das Europäische Parlament mit überwältigender Mehrheit am 15. April verabschiedet wurde: 626 Ja-Stimmen, von 687 abgegebenen Stimmen, bei 45 Gegenstimmen und 16 Enthaltungen. Die Verordnung wurde vom Europäischen Parlament und dem Rat der Europäischen Union am 21. Mai 2013 ratifiziert.

Die neue Verordnung bestätigt ENISAs erreichte Leistungen in Bereichen wie Computernotfallteams (Computer Emergency Response Teams (CERT)) in den Mitgliedstaaten und seinen Weltklasse-Internet-Sicherheitsübungen wie Cyber Europe 2012, mit 600 Teilnehmern aus ganz Europa.

Weitere wichtige Punkte der neuen Verordnung beinhalten:

- Die Bereitstellung einer starken Schnittstelle bei der Bekämpfung der Internetkriminalität – mit einem Schwerpunkt auf Prävention und Erkennung – mit dem europäischen Zentrum gegen Internet-Kriminalität (Cybercrime Europol Center (EC3))
- Die Unterstützung von ENISA bei der Entwicklung der EU-Internet-Sicherheitspolitik und -gesetzgebung
- Die Unterstützung der Agentur bei der Forschung, Entwicklung und Standardisierung, mit EU-Richtlinien für Risikomanagement und Sicherheit von elektronischen Produkten, Netzwerken und Dienstleistungen
- ENISAs Unterstützung bei der Prävention und Erkennung von sowie Reaktion auf grenzüberschreitende Bedrohungen im Internet
- Die engere Ausrichtung von ENISA an das EU-Kontrollverfahren durch Unterstützung und Beratung für EU-Länder und Institutionen

Die Verordnung bestätigt zudem, dass der Agentursitz (Hauptsitz) in Heraklion auf Kreta bleibt, mit einem operativen Zweitsitz in Athen.

Die im Februar veröffentlichten EU-Internet-Sicherheitsstrategie und -richtlinie, sprechen ENISA ebenfalls eine Schlüsselrolle beim Schutz der europäischen Internetlandschaft zu.

Die EU-Cybersicherheitsstrategie braucht Vertrauen und den Schutz der Privatsphäre

Cybersicherheit ist keine Entschuldigung für die unbegrenzte Überwachung und Analyse persönlicher Daten, so der Europäische Datenschutzbeauftragte Peter Hustinx am 17.06.2013 aus Anlass der Veröffentlichung seiner Stellungnahme[1] zur Cybersicherheitsstrategie der Europäischen Union[2]. Die Strategie enthält zwar eine willkommene Bestätigung der Wichtigkeit der Datenschutzprinzipien, sie ist allerdings unklar bezüglich der Frage, wie diese Prinzipien in der Praxis umgesetzt werden sollen, um die Sicherheit von Personen, Unternehmen, Regierungen und anderen Organisationen zu schützen.

Das allgemeine Ziel der EU-Strategie ist es, die Nutzung des Internets und aller mit ihm verbundenen Netzwerke und Informationssysteme sicherer zu machen, indem Organisation in den EU-Staaten dazu befähigt werden, Störungen und Cyber-Angriffe zu verhindern und auf sie zu reagieren. Das Ergebnis soll ein größeres Vertrauen von Personen und Organisationen in das Internet sein. Die Mitteilung der Kommission beachtet allerdings nicht genügend die Rolle des Datenschutzrechts und aktueller EU-Rechtsetzungsvorschläge, wie etwa der vorgeschlagenen Datenschutzgrundverordnung und der e-Trust-Verordnung bei der Förderung der Cybersicherheit. Sie ignoriert ebenfalls, wie wichtig es ist, den Datenschutz bereits in der Entwicklung von Systemen, die der Cybersicherheit dienen sollen, zu berücksichtigen – eingebauter Datenschutz -, um ein Fundament für Vertrauen zu schaffen.

Die Folge ist, dass die Strategie nicht so effektiv und umfassend ist, wie die Kommission beabsichtigte.

Zwar können Maßnahmen zur Cybersicherheit die Analyse bestimmter personenbezogener Daten, wie etwa IP-Adressen, die zu

1 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf

2 http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security