**Originaltext aus dem Koalitionsvertrag von CDU, CSU und SPD zum Thema „IT-Infrastruktur und digitaler Datenschutz“**

Wir schaffen ein IT-Sicherheitsgesetz mit verbindlichen Mindestanforderungen an die IT-Sicherheit für die kritischen Infrastrukturen und der Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle. Dafür setzen wir uns auch auf der EU-Ebene im Rahmen der europäischen Cybersicherheitsstrategie ein.

Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.

Wir bauen die Kapazitäten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und auch des Cyber-Abwehrzentrums aus. Wir verbessern die IT-Ausstattung der deutschen Sicherheitsbehörden.

Um Bürgerdaten besser zu schützen und zu sichern, werden wir die Bündelung der IT-Netze des Bundes in einer einheitlichen Plattform „Netze des Bundes“ anstreben. IT- und TK-Sicherheit wollen wir zusammenführen.

Die Bundesbehörden werden verpflichtet, zehn Prozent ihrer IT-Budgets für die Sicherheit ihrer Systeme zu verwenden.

Um Vertrauen wieder herzustellen müssen die Standardisierungsgremien transparenter werden. Zudem muss sich Deutschland stärker in diesen und anderen internationalen Gremien beteiligen, besonders solchen der Internetarchitektur und Internet-Governance.

Wir prüfen, inwieweit ein Ausverkauf von nationaler Expertise und Know-how in Sicherheits-Schlüsseltechnologien verhindert werden kann.

Wir initiieren ein Spitzencluster „IT-Sicherheit und kritische IT-Infrastruktur“.

Um zu gewährleisten, dass die Nutzerinnen und Nutzer über die Sicherheitsrisiken ausreichend informiert sind, sollen Internetprovider ihren Kunden melden, wenn sie Hinweise auf Schadprogramme oder ähnliches haben. Darüber hinaus streben wir einen sicheren Rechtsrahmen und eine Zertifizierung für Cloud-Infrastrukturen und andere sicherheitsrelevante Systeme und Dienste an.

Zur Wahrung der technologischen Souveränität fördern wir den Einsatz national entwickelter IT-Sicherheitstechnologien bei den Bürgerinnen und Bürgern.

Die Weiterentwicklung und Verbreitung von Chipkartenlesegeräten, Kryptographie, DE-Mail und sicheren Ende-zu-Ende-Verschlüsselungen sowie vertrauenswürdiger Hard- und Software gilt es erheblich auszubauen. IT-Hersteller und -Diensteanbieter sollen für Datenschutz- und IT-Sicherheitsmängel ihrer Produkte haften.

Wir wollen das vom Bundesverfassungsgericht entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme mit Leben füllen. Die Nutzung von Methoden zur Anonymisierung, Pseudonymisierung und Datensparsamkeit müssen zu verbindlichen Regelwerken werden.

Wir werden den technikgestützten Datenschutz („Privacy by Design“) und den Datenschutz durch Voreinstellungen („Privacy by Default“) ausbauen.

Um die Grund- und Freiheitsrechte der Bürgerinnen und der Bürger auch in der digitalen Welt zu wahren und die Chancen für die demokratischen Teilhabe der Bevölkerung am weltweiten Kommunikationsnetz zu fördern, setzen wir uns für ein Völkerrecht des Netzes ein, damit die Grundrechte auch in der digitalen Welt gelten. Das Recht auf Privatsphäre, das im Internationalen Pakt für bürgerliche und politische Rechte garantiert ist, ist an die Bedürfnisse des digitalen Zeitalters anzupassen.