TÜV®

# VdTÜV-Eckpunktepapier zur Errichtung einer Stiftung Datenschutz

Informationstechnik mit digitaler Datenverarbeitung und Datenübermittlung entwickelt sich grenzüberschreitend und erfasst mittlerweile nahezu alle Lebensbereiche der Bürgerinnen und Bürger. Deswegen ist eine intensive ordnungspolitische Fokussierung auf die Anforderungen des Datenschutzes erforderlich.

Eine Stiftung Datenschutz könnte als leistungsfähige Koordinierungsinstanz sowohl für die Belange hoheitlicher Datenschutzpflichten eintreten, als auch die dem Datenschutz dienenden privatwirtschaftlichen Beiträge der betroffenen Wirtschaftsakteure flankierend unterstützen.

## Markt- und Bürgervertrauen durch Transparenz

So sollte die Stiftung Datenschutz auf eine einheitliche Interpretation datenschutzrechtlicher Sachverhalte durch staatliche Akteure (Landesdatenschutzzentren-, behörden-, beauftragten, Bundesdatenschutzbeauftragter etc.), private Prüf- und Zertifizierungsstellen sowie betroffene Unternehmen hinwirken. Oberstes Ziel dieser Anstrengungen muss Markt- und Bürgervertrauen durch entsprechende Datenschutztransparenz bei Produkten, Dienstleistungen, Unternehmen und relevanten Prozessen insbesondere der Informations- und Kommunikationstechnik bilden.

## TÜV können engagiert begleiten

Die durch den VdTÜV e.V. vertretenen TÜV-Unternehmen sind bereit und in der Lage, mit ihrer Kompetenz und ihren einschlägigen freiwirtschaftlichen Dienstleistungen im Bereich Datenschutz und Informationssicherheit die Aktivitäten einer solchen Koordinierungsinstanz engagiert zu begleiten und ihre Zielsetzungen zu fördern.

## Sieben Eckpunkte für Stiftung Datenschutz

Für die Errichtung einer Stiftung Datenschutz sollten folgende sieben Eckpunkte Berücksichtigung finden:

1.) Die Stiftung Datenschutz sollte eine leistungsfähige Koordinierungsinstanz in dem Prozess der Erarbeitung eines einheitlichen Prüf- und Zertifizierungsregelwerks werden und privatwirtschaftliche Beiträge der betroffenen Wirtschaftsakteure flankierend unterstützen. Die operative Umsetzung des Regelwerks erfordert die Leistungskraft etablierter Wirtschaftsakteure. Die Vergabe von freiwilligen Prüfzeichen durch unabhängige Dritte sowie die Durchführung entsprechender Zertifizierungsverfahren im Bereich des Datenschutzes stellt eine klassische freiwirtschaftliche Dienstleistung im Wettbewerb dar. Diese ist bereits heute hoheitlicher Aufsicht unterstellt.

## Unabhängigkeit und Neutralität sind sichergestellt

Gemäß den einschlägigen gesetzlichen Vorgaben wird die Unabhängigkeit, Neutralität und Fachkompetenz der involvierten privaten Prüforganisationen durch das nationale Akkreditierungsverfahren sichergestellt. Diese Aufgabe obliegt in Deutschland der Deutschen Akkreditierungsstelle GmbH

(DAkkS). Für den Bereich des Datenschutzes fehlen dort bislang einheitliche Akkreditierungsverfahren, worauf – eventuell in Zusammenarbeit mit der Stiftung Datenschutz – hingearbeitet werden sollte.

Dezentraler Systemansatz

Aufgrund positiver Erfahrungen wird auch in anderen hochsensiblen Sicherheitsbereichen, so beispielsweise in den Sektoren der Anlagen- und Fahrzeugsicherheit sowie im Rahmen der gesetzlich verankerten „GS-Zeichen"-Vergabe, auf die Leistungsfähigkeit privatwirtschaftlich getragener und organisierter Modelle vertraut, d.h. auf die Dienstleistungen akkreditierter unabhängiger Prüf- und Zertifizierungsinstitutionen. An diesem bewährten dezentralen, marktorientierten und wettbewerbsoffenen Systemansatz sollte auch in punkto Datenschutz festgehalten werden.

Einheitliche Kriterien

Unter vorgenannten Rahmenbedingungen sollte die Stiftung Datenschutz einheitliche Kriterien sowie Audit- und Zertifizierungsverfahren entwickeln, aber nicht selbst durchführen. Einheitliche Kriterien und Anforderungen können in einem weiteren Schritt zur Definition und Implementierung eines Gütesiegels unter Einbindung der betroffenen Wirtschaftsakteure führen. Die visuellen Gestaltung und das Vergabesystem eines einheitlichen Gütesiegels sollten ebenfalls in Anlehnung an das GS-Zeichensystem erfolgen.

Enge Kooperation

2.) Soweit die Stiftung Datenschutz damit betraut würde, die Entwicklung normierter Datenschutzanforderungen für Produkte, Dienstleistungen und Unternehmen weiter voranzutreiben, sollte sie hierbei mit den entsprechenden nationalen, europäischen und internationalen Behörden und Normungsorganisationen äußerst eng kooperieren. Für die Gewährleistung der Transparenz und Vergleichbarkeit der Prüfaussagen ist es unerlässlich, einheitliche Kriterien und eine gemeinsame Interpretation der vordringlich relevanten datenschutzrechtlichen Sachverhalte unter Einbeziehung der Aufsichtsbehörden, Normungsorganisationen, Prüf- und Zertifizierungsstellen sowie Verbraucherschützer und Unternehmen herbeizuführen. Auch müssten die internationalen Initiativen der relevanten Datenschutzgremien zur Schaffung von internationalen Datenschutzstandards berücksichtigt werden.

Echter Mehrwert der Datenschutz-Zertifikate

Die Stiftung sollte sich in die Arbeiten bei den Normungsorganisationen einbringen, um die Kompatibilität zu den bereits existierenden bzw. sich in Abstimmungsprozessen befindlichen einschlägigen Normenreihen (wie, z.B. die ISO-Normenreihe 29100) zu gewährleisten und somit zu einem echten Mehrwert der Datenschutz-Zertifikate beizutragen. Durch die Förderung des offenen wechselseitigen Dialogs und Gedankenaustauschs der Datenschutz-Community sollten die Optimierungspotentiale im Bereich Datenschutz erkannt und ausgeschöpft werden.

Stärkere Akzeptanz der Vorgaben

Identifizierte Lösungsansätze müssen insbesondere auch für die europäische und internationale Diskussion fruchtbar gemacht werden. Darüber hinaus sollte dies dazu führen, dass im Marktgeschehen und bei den Verbrauchern eine stärkere Akzeptanz für die Einhaltung datenschutzrechtlicher Vorgaben und die freiwillige Nachfrage für entsprechende unabhängige Überprüfungen erzeugt wird.

Normativer Rahmen für Zertifizierung

3.) Die EU-Kommission strebt aktuell ausweislich der Mitteilung vom 4. November 2010 (KOM (2010) 609 final) ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ an. Notwendig sind europaweit gleiche Voraussetzungen, die den Verbrauchern Sicherheit geben und praktische Lösungen für Unternehmen bieten. Insbesondere prüft die EU-Kommission auf Empfehlung der Art.29-Datenschutzgruppe die Möglichkeit zur Einführung von EU-Zertifizierungsregelungen (z. B. Europäisches Datenschutzsiegel) für Verfahren, Technologien, Produkte und Dienste. In seiner Stellungnahme weist das Expertengremium darauf hin, dass – im Hinblick auf die Schlüsselrolle solcher Zertifizierungsprogramme im Binnenmarkt und das damit einhergehende Gebot zur Aufrechterhaltung hoher Qualität der Verfahren – die Schaffung eines normativen Rahmens für die Erbringung der Zertifizierungsleistungen unerlässlich ist.

EU-Ebene im Blick behalten

Durch einheitliche Prozeduren soll der aus den anderen Bereichen bekannten Lockerung der Verfahren vorgebeugt werden. Die nationalen Datenschutzaktivitäten – wie die Stiftung Datenschutz – sind hinsichtlich der Entwicklungen auf der EU-Ebene u. a. im Bereich EU-Telekommunikationsvorschriften fortlaufend zu analysieren, da sich daraus ggf. die Notwendigkeit der Anpassung des Aufgabenzuschnitts und der vorrangigen Arbeitsschwerpunkte der Stiftung ergeben kann.

Allenfalls Datenschutzfreundlichkeit kann geprüft werden

4.) Vergleichende Prüfungen von Produkten und Dienstleistungen durch die Stiftung Datenschutz erscheinen grundsätzlich nicht Ziel führend und wecken überzogene Erwartungen. Datenschutzprüfungen im Sinne vergleichender Tests müssten so ausgelegt werden, dass sie repräsentativ sind und deren Vergleichbarkeit gewahrt ist. Im Rahmen dieser Tests kann allenfalls die Datenschutzfreundlichkeit und nicht die Datenschutzkonformität der Produkte und Dienstleistungen geprüft werden.

Vergleichstests sind nicht realistisch

Die sich daraus in den Prüfaussagen ergebenden Unterschiede müssten den Betroffenen transparent gemacht werden. Die Einhaltung der Anforderungen der Datenschutzgesetzgebung ist bei IT-Programmen, IT-Systemen, Internet- Handelsplattformen usw. nur durch sehr aufwendige Prüfungen bzw. Audits sowie unter bestimmten datenschutzrelevanten Einzelaspekten festzustellen. Solche Prüfungen sollten den darin bereits erfahrenen Prüforganisationen überlassen bleiben. Hinzu kommt, dass eine Stiftung Datenschutz die Unternehmen nicht dazu zwingen kann, ihre unternehmensinternen datenschutzrelevanten Prozesse offenzulegen. Somit sind aussagekräftige, in die Tiefe gehende Vergleichstests insgesamt nicht realistisch.

Einschlägige Datenschutzgesetze

Im Wesentlichen lässt sich nur die Einhaltung der gesetzlich vorgeschriebenen Transparenz- und Einwilligungsanforderungen ohne Mitwirkung der Anbieter überprüfen. Die faktische Ausgestaltung der IT-Dienstleistungen ist einer unaufgeforderten Prüfung – nach dem hier angestrebten Vorbild der Stiftung Warentest – nicht zugänglich. Eine vollumfängliche Datenschutzanalyse erfolgt jeweils unter Anwendung der für den konkreten Prüfgegenstand einschlägigen Datenschutzgesetze. Sie umfasst die eingehende Bewertung der Zulässigkeit der Datenverarbeitung und der Angemessenheit der getroffenen technisch-organisatorischen Maßnahmen. Hierfür sind weitere, über die allgemein zugänglichen

Informationen hinausgehende Angaben erforderlich. Eine Prüfung der Datenschutzkonformität mit dem Ansatz der vergleichenden Tests ist ausgeschlossen.

Freiwillige Audits zielen auf Datenschutzkonformität ab

Im Gegensatz zu den Tests zielt der Prüfansatz der freiwilligen Audits auf die Bestätigung der Datenschutzkonformität ab. Die Unterschiede müssten der Öffentlichkeit transparent gemacht werden, damit nicht der Eindruck entsteht, beide Verfahren seien in ihren Prüfaussagen gleichzusetzen. Hier müsste differenziert werden zwischen der Bescheinigung von Datenschutzfreundlichkeit, die durch vergleichende Tests möglich ist, und Datenschutzkonformität, deren Bestätigung nur unter Anwendung von geeigneten Prüfansätzen möglich ist. Es wäre daran zu denken, dass eine Stiftung Datenschutz der Stiftung Warentest selbst ggf. durch punktuelle Hilfestellung bei der Umsetzung entsprechender Zielvorstellungen, d.h. bei der vergleichenden Prüfung von Produkten und IT-basierten Systemen im Hinblick auf die Einhaltung der Transparenz- und Informationspflichten, Unterstützung leistet.

Aufklärungs- und Informationsangebote

5.) Die Stiftung Datenschutz sollte sich im Arbeitsschwerpunkt zunächst darauf konzentrieren, Aufklärungs- und Informationsangebote im Bereich Datenschutz bereitzustellen. Sie sollte hierbei neben Unternehmern insbesondere auch die betroffenen Bürger für die Belange des Datenschutzes nachhaltig sensibilisieren und ihnen praktische Handlungsempfehlungen im Sinne des Verbraucherschutzes geben, damit diese sich in puncto Datenschutz sicherer in der komplexen IT-Welt bewegen können. Es geht hierbei vor allem auch darum, den Selbstdatenschutz durch Aufklärung deutlich zu verbessern.

Datenschutz sollte in Prozesse implementiert sein

6.) Die Stiftung Datenschutz sollte Unternehmen durch entsprechende Informations- und Schulungsangebote dazu anregen, Datenschutzanforderungen in ihren Prozessen und IT-Anwendungen präventiv zu implementieren. Auch hier gibt es Bestrebungen auf EU-Ebene, die Umsetzung der Datenschutzgrundsätze in die internen Prozesse der Unternehmen durch die Einführung der sog. Rechenschaftspflicht sicherzustellen. Durch das Erarbeiten von Best Practices kann die Stiftung Hilfestellungen für die Unternehmen geben. Hierbei sollte sie insbesondere auch die deutlichen Vorteile kommunizieren, welche unter transparenter Dokumentation von unabhängigen Dritten vergebene freiwillige Prüfzeichen und Zertifikate bieten. Sie sollte vermitteln, dass nach außen hin dokumentierter Datenschutz einen qualitativen Wettbewerbsvorteil und mehr Rechtssicherheit bietet.

Koordinierung von Forschungsprojekten

7.) Einen zusätzlichen zentralen Arbeitsschwerpunkt der Stiftung Datenschutz sollte die Koordinierung und Initiierung von Forschungsprojekten im Bereich Datenschutz bilden. Hierbei wird man sich insbesondere darauf konzentrieren müssen, zukunftsorientierte Lösungsansätze für die technologischen Herausforderungen sowie tragfähige Ansätze und konkrete Vorschläge für eine Modernisierung des deutschen und europäischen Datenschutzrechts zu entwickeln.