DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Requirements for data protection and IT security law regarding technology development

Martin Schallbruch

Issue 2, 2017

In December 2016, the Digital Society Institute hosted a workshop on requirements to create a compatibility of data protection and IT security regulation. Contributions to the workshop were given by Marit Hansen (ULD Schleswig-Holstein), Tomasz Lawicki (TeleTrusT working group "State of the Art Technology"), Steve Ritter (BSI) and Johannes Schlattmann (LVM).

1. Current state of affairs

Basic findings

Data protection and IT security laws have common roots in constitutional law and are mostly not differentiated in the public view (nor, to a degree, in the political sphere). However, legislation at the European and national levels differ significantly. In particular, data protection, which is closely aligned to the protection of individual rights, addresses the individual person, while IT security law takes a rather systemic view (i.e., protecting critical infrastructures, requirements for "harmful" technical systems). Corresponding to their respective protective goals, both legal fields claim to influence technical development and technology-driven business model innovation.

The development of legal requirements for technology

Over the last two years, the legal infrastructures governing both data protection and IT security have evolved substantially, which has further implications for the design of technology. Under EU General Data Protection Regulation (GDPR), technological requirements have not fundamentally changed, but there has been a tightening of procedural rules and sanctions. Specifically in IT security law there are new technical requirements for certain businesses: critical infrastructure operators and, under the NIS Directive, digital service providers.

Both legislations barely define data protection and IT security technologies, and are limited to specific objectives and the need to implement "state of the art" technical measures. Furthermore, the legislation does not define an absolute level of protection, but rather an appropriate protection in relation to the given risks.

The extension of the requirement and the stronger demand and sanctioning are an opportunity for technical data protection ("privacy-by-design") and for more effective IT security. The implementation of the new legal norms could be a stimulus for technological innovation.

Conflicts of interest between IT security and data protection

Current approaches to filtering, advanced detection, and active cybersecurity are heavily based on the extensive storage and analysis of communication data as a means for early detection of cyberattacks or data leaks.

CIOs of IT user companies complain that German data protection laws only allow limited use of current products for cybersecurity, but this assessment has not been objectively verified. In particular, it is not yet clear whether data protection-compliant procedures (e.g., pseudonymization) are sufficient for current security strategies, and whether they comply with data protection regulations. More research is required at this point.

Such conflicts between data protection and IT security only emerge because current security approaches are focused on detection paradigms. An increase in more basic security standards, reducing vulnerability and attack vectors through stronger architecture, high assurance systems, and the improvement of methods to measure and evaluate security, would reduce the need for storing and analyzing communication data, and thus remove the conflicts between data protection and IT security.

Compatibility of IT security and data protection requirements

The technical requirements of data protection and IT security are of equal importance. However, sound IT security is only a necessary condition for reliable data protection, not a sufficient one. The extensive objectives of data protection typically add additional requirements for data avoidance and data minimization. Overall, the definition of IT security requirements, their verifiability, and their verification are more mature than for data protection, due to their longer history, the strong role of written "basic security" catalogues, and international standards.

Beyond specific technical requirements, data protection and IT security generally have separately-defined standards for management systems (e.g., ISO 27001 for IT security and the German "Standard-Datenschutzmodell" for data protection). Accordingly, management systems in companies are also generally separated, with different parties responsible for each. This separation of responsibilities isn't necessarily without problems, but can help when addressing conflicts of interest between the responsible parties, and can even generate constructive competition.

Independent data protection authorities and the Federal Agency for Information Security (BSI) serve an advisory role and contribute towards defining the "state of the art" technology, which is ultimately determined by courts. On the other hand, data protection authorities and BSI, given their legal foundations, perform a much stronger authorization function than earlier, as they stipulate the penalties and adequacy of technical measures themselves.

2. Recommendations

Recommendations for companies

IT security and data protection governance – separate but linked

Companies should define and implement separate management systems for both. But since data protection and IT security address a large amount of overlapping issues, the respective strategies and management systems should be procedurally linked, and, in the context of the company's mission, balanced.

Strive for high technical standards

New regulation requires that, in principle, technical means should assure a high level of protection. At the same time, the risks of cyberthreats in an ever more connected world are increasing. Therefore, measures of data protection and IT security should be as strong as possible, even in areas that have not yet been regulated. Thus, well-elaborated and demanding risk assessments should be pursued.

Policy recommendations

Incentives rather than detailed regulation

Adequate technical measures for data protection and IT security objectives cannot be achieved through more detailed regulation. Rather, a system that incentivizes such measures is necessary. Two basic approaches seem particularly helpful: (a) coupling legal responsibility such as liability with corresponding insurance models; and, (b) strengthening the demand side through quality seals, labels, certification, etc. Quality seals must be based on measurable contributions towards attaining security objectives; they should not solely be based on simple and generic baseline characteristics.

Transparency and the measurement of risks and damage

The choice of risk-appropriate technical measures in companies can be more robust if the risks of data protection and IT security incidents are made transparent and measurable. A practice-oriented development of applicable methods for risk assessment should be encouraged. Risks should be defined as broadly as possible, and larger risks for society need to be covered as well.

Support of open industry standards for "state of the art" definitions

The industry-based development of definitions of "state of the art" technology (such as the recommendation by TeleTrusT e.V.) can help to establish acceptable technical implementations of legal requirements and industry-to-industry assistance. To be effective, such industry standards must be developed in an open process which can adapt to technological change.

Cooperation in official recommendations

Independent data protection authorities and the BSI, should work together more closely. Standard data protection models and baseline IT security as well as the publication of recommendations should be coordinated between them, involving companies and academia. At the very least, for points of overlapping relevance, mutual cross-reference is needed. This will also increase the chances for implementation among companies.

Pragmatic modular recommendations

Comprehensive standardization in data protection and IT security is neither probable nor desirable. State privacy and IT security officers should rather create business model- or technology-specific recommendations addressing concrete problems (e.g., household appliances, fitness machines, cars, medical technology, etc.), which combine data protection and IT security requirements. Such recommendations can also be used to foster standardization.

Exchange between privacy and IT security

An exchange between key institutional stakeholders – through common organizations, exchange formats, repositories, etc. – is desirable, and could begin through joint venture projects.

The DSI Industrial & Policy Recommendations (IPR) Series is published by the Digital Society Institute of ESMT Berlin, http://dsi.esmt.org.

DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Anforderungen des Datenschutzes und der IT-Sicherheit an die Gestaltung von Technik

Martin Schallbruch

Ausgabe 2, 2017

Im Dezember 2016 war das Digital Society Institute Gastgeber für einen Workshop zu der Vereinbarkeit von Anforderungen des Datenschutzes und der IT-Sicherheit an die Gestaltung von Technik. Impulse zu dem Workshop steuerten Marit Hansen (ULD Schleswig-Holstein), Tomasz Lawicki (TeleTrusT AG „Stand der Technik), Steve Ritter (BSI) und Johannes Schlattmann (LVM) bei.

1. Sachstand

Ausgangslage

Datenschutz und IT-Sicherheit haben gemeinsame verfassungsrechtliche Grundlagen und werden auch im Problembewusstsein der Öffentlichkeit (und Teilen der Politik) nicht unterschieden. Die einfachrechtliche Ausgestaltung auf europäischer und nationaler Ebene unterscheidet sich jedoch erheblich. Insbesondere nimmt das vom Individualrechtsschutz kommende Datenschutzrecht überwiegend den Blickwinkel des Betroffenen ein, während das IT-Sicherheitsrecht in der Regel eine eher systemische Sichtweise praktiziert (Schutz kritischer Infrastrukturen, Vorgaben für „gefährliche“ Systeme). Bei der Ausgestaltung der Anforderungen an Technologie und Geschäftsmodelle berühren sich beide Rechtsmaterien und treffen spätestens bei der Adressierung konkreter Systeme und spezifischer technischer Vorgaben zusammen. Beide Rechtsgebiete erheben den Anspruch der Einflussnahme auf technische Entwicklung und technologisch getriebene Geschäftsmodellinnovation im Sinne ihrer jeweiligen Schutzziele.

Entwicklung der rechtlichen Anforderungen an Technik

Sowohl das Datenschutzrecht als auch das IT-Sicherheitsrecht haben in den letzten zwei Jahren grundlegende Weiterentwicklungen erfahren, die auch die Anforderungen an Technologie betreffen. Im Datenschutzrecht (Datenschutzgrundverordnung) sind die Anforderungen an Technologie keine grundsätzlich anderen als in der Vergangenheit, allerdings ist mit der Verschärfung der Verfahrensvorschriften und den eingeführten Sanktionen ein stärkerer Umsetzungsdruck entstanden. Im IT-Sicherheitsrecht finden sich neue technische Anforderungen für bestimmte Gruppen von Anwendern, kritische Infrastrukturbetreiber oder – mit der NIS-Richtlinie – auch digitale Diensteanbieter.

Beide Rechtsmaterien verzichten auf eine Definition einzusetzender Datenschutz- bzw. IT- Sicherheitstechnologien und beschränken sich auf Datenschutz- und IT-Sicherheitsziele und das Erfordernis, dem „Stand der Technik“ entsprechende Maßnahmen zu ergreifen. Hierbei wird jedoch in den Rechtsvorschriften kein absolutes Schutzniveau definiert, sondern ein dem jeweiligen Risiko angemessener Schutz verlangt.

Die Erweiterung der Anforderung bzw. stärkere Einforderung und Sanktionierung ist eine Chance für

den technischen Datenschutz („privacy-by-design“) und für wirksamere IT-Sicherheit. Mit der Implementierung der neuen Rechtsnormen könnte ein Schub an technologischer Innovation einhergehen.

Interessengegensätze zwischen IT-Sicherheit und Datenschutz

Aktuelle Ansätze zur Cyberabwehr setzen stark auf die sehr weitgehende Speicherung von Kommunikationsdaten als Grundlage für das frühzeitige Erkennen der Vorbereitung von Cyberangriffen oder von beginnenden Datenabflüssen. Aus Sicht der CIO von Anwenderunternehmen lässt das deutsche Datenschutzrecht den Einsatz aktueller Produkte zur Cyberabwehr nur eingeschränkt zu. Diese Einschätzung ist bislang nur schwach belegt. Insbesondere ist noch nicht ausreichend geklärt, ob datenschutzkonforme Verfahrensweisen (etwa der Pseudonymisierung) ausreichen, um einerseits aktuelle Verteidigungsstrategien umzusetzen und andererseits die datenschutzrechtlichen Regelungen einzuhalten. Hier besteht Forschungsbedarf.

Diese möglicherweise bestehenden Interessengegensätze zwischen Datenschutz und IT- Sicherheit bestehen insgesamt grundsätzlich nur, solange die derzeitigen Systemarchitekturen, Entwicklungswerkzeuge und Einsatzformen Schwachstellen-gestützte Angriffe zulassen. Eine Erhöhung des Sicherheitsniveaus durch härtere Architekturen und High Assurance Systeme sowie die Verbesserung der Mess- und Evaluierbarkeit der Sicherheit von Systemen verringert die Notwendigkeit, Kommunikationsdaten zu speichern und damit den Interessengegensatz zwischen Datenschutz und IT-Sicherheit.

Vereinbarkeit von Anforderungen der IT-Sicherheit und des Datenschutzes

Die Anforderungen aus dem Datenschutzrecht an die Technikgestaltung und die Anforderungen aus dem IT-Sicherheitsrecht stehen gleichrangig nebeneinander. In der Tendenz ist die Erfüllung von Anforderungen der IT-Sicherheit notwendige Bedingung für die Erfüllung von Anforderungen des Datenschutzes, aber aus Sicht des Datenschutzes oftmals nicht ausreichend. Wegen der erweiterten Schutzziele des Datenschutzes kommen typischerweise weitere Anforderungen hinzu, um etwa Datensparsamkeit sicherzustellen. Insgesamt ist die Definition von Anforderungen der IT-Sicherheit, ihre Prüfbarkeit und ihre Prüfung wegen der längeren Vorgeschichte und der starken Rolle des IT-Grundschutzes und entsprechender internationaler Normen auf einem höheren Reifegrad als beim Datenschutz.

Oberhalb der konkreten technischen Anforderungen bestehen im Datenschutz und in der IT- Sicherheit getrennt definierte Anforderungen an Managementsysteme (z.B. ISO 27001 für IT-Sicherheit und Standard-Datenschutzmodell für Datenschutz). Demzufolge sind die Managementsysteme in den Unternehmen getrennt und auch bei verschiedenen Verantwortlichen angesiedelt. Diese Trennung von Zuständigkeiten ist wegen der überschneidenden Materien nicht unproblematisch, hilft aber in Fällen von Interessengegensätzen zu einer adäquaten Auseinandersetzung der Entscheider mit den Sichtweisen der verschiedenen Bereiche und kann einen konstruktiven Wettbewerb erzeugen.

Unabhängige Datenschutzbehörden und BSI haben einerseits beratende Funktion und wirken mit ihren Beiträgen bei der Definition des Standes der Technik, der letztlich durch die Rechtsprechung erfolgt, mit. Andererseits haben Datenschutzbehörden und BSI aufgrund ihrer Rechtsgrundlagen weit stärker als früher eine genehmigungsähnliche Funktion, weil sie Sanktionen verhängen können und hierbei die Angemessenheit der technischen Maßnahmen selbst beurteilen.

2. Empfehlungen

Empfehlungen an Unternehmen

IT-Sicherheits- und Datenschutz-Governance getrennt, aber verknüpft

Für beide Bereiche ist im Unternehmen jeweils ein eigenständiges Managementsystem zu definieren und zu implementieren. Da Datenschutz und IT-Sicherheit im Unternehmen zu einem hohen Prozentsatz überschneidende Materien betreffen, müssen die jeweiligen Strategien und Managementsysteme prozedural verknüpft und im Kontext des Unternehmenszweckes ausbalanciert werden.

Hohes technisches Niveau anstreben

Neuere Regulierung verlangt beim Stand der Technik grundsätzlich ein hohes Niveau. Gleichzeitig steigen die Risiken durch Vernetzung und Cyber-Bedrohung weiter an. Daher sollten sich Maßnahmen zu Datenschutz und IT- Sicherheit auch in den noch nicht regulierten Bereichen am höchsten praktisch erprobten Niveau orientieren. Dabei ist ein möglichst belastbares Risiko-Assessment zu Grunde zu legen.

Empfehlungen an die Politik

Incentivierung statt detailliertere Regulierung

Adäquate technische Maßnahmen zur Erfüllung von Datenschutz- und IT-Sicherheitszielen können nicht durch detailliertere Regulierung erreicht werden. Vielmehr ist ein System der Incentivierung solcher Maßnahmen notwendig. Hierfür bestehen zwei grundsätzliche Ansatzpunkte: (a) Rechtliche Förderung von Verantwortungsübernahme/Haftung und entsprechenden Versicherungsmodellen sowie (b) Stärkung der Nachfrageseite durch Gütesiegel, Label, Zertifizierung etc. Gütesiegel müssen messbare Beiträge zur Erreichung der Schutzziele bestätigen; sie dürfen nicht bloße Formalanforderungen abbilden.

Förderung von Transparenz und Messbarkeit von Risiken und Schäden:

Die Auswahl risikoangemessener technischer Maßnahmen in den Unternehmen kann belastbarer gestaltet werden, wenn die Risiken und Schäden von Datenschutz- und IT-Sicherheitsvorfällen transparenter gemacht und gemessen werden. Die praxisorientierte Entwicklung entsprechender Methoden sollte gefördert werden. Hierbei ist ein sehr weitgefasster Risiko-Begriff zu Grunde zu legen, weil auch gesamtgesellschaftliche Risiken erfasst werden müssen.

Unterstützung von offenen Branchenstandards zur Dokumentation des Standes der Technik

Die Entwicklung von Branchenstandards zur Definition des Standes der Technik (wie der Handreichung „Stand der Technik“ des TeleTrusT e.V.) durch die Unternehmen selbst kann unternehmensübergreifend Hilfestellung geben, wie die rechtlichen Anforderungen konform technisch umzusetzen sind. Um belastbare Wirkung zu entfalten, müssen solche Branchenstandards in offenen Prozessen erstellt werden, um die Technikinnovation abzubilden.

Verschränkung behördlicher Empfehlungen und Vorgaben

Unabhängige Datenschutzbehörden und BSI mit ihrer gewandelten Rolle sollten ihre Tätigkeit stärker miteinander verschränken. Die Weiterentwicklung von Standard-Datenschutzmodell und IT- Grundschutz oder auch die Herausgabe von Empfehlungen und Handreichungen sollten abgestimmt und unter Einbeziehung der Unternehmen und der Wissenschaft erfolgen. Mindestens an relevanten Stellen sollte wechselseitig aufeinander verwiesen werden. Damit wird die Umsetzungschance bei den Unternehmen erhöht.

Förderung pragmatischer modularer Empfehlungen

Eine umfassende Vereinheitlichung der Anforderungskataloge und Managementsysteme im Datenschutz und in der IT-Sicherheit ist weder wahrscheinlich noch in toto wünschenswert. Staatliche Datenschutz- und IT- Sicherheitsverantwortliche sollten vielmehr Anwendungs-, Geschäftsmodell- oder Technologiespezifische Handreichungen und Empfehlungen fördern, die für konkrete Problemlagen (z.B. Haushaltsgeräte, Fitnesstracker, Autos, Medizintechnik usw.) zusammengefasste Anforderungen aus Datenschutz und IT-Sicherheit definieren. Solche Handreichungen können auch in die Standardisierung eingebracht werden.

Austauschorganisation Datenschutz und IT-Sicherheit

Eine institutionelle Verschränkung der Verantwortungsträger durch gemeinsame Organisationen, Austauschformate, Repositories etc. ist wünschenswert und könnte über gemeinsame Projekte begonnen werden.

Die DSI Industrial & Policy Recommendations (IPR) Series wird herausgegeben vom Digital Society Institute der ESMT Berlin, http://dsi.esmt.org.