Transformation
Consulting
International

Compliance mit der DSGVO
Stand der Technik - Wie gehen wir mit Artikel 32 der DSGVO um?

Entscheidend für den Erfolg der Umsetzung der EU-DSGVO ist der „geschickte“ initiale Einstieg in die Fülle von erforderlichen Maßnahmen und in die Rechenschafts- und Nachweispflicht.

Holger Schellhaas

München, Januar 2018

Transformation Consulting International

Sicherheit der Verarbeitung nach Artikel 32 DSGV

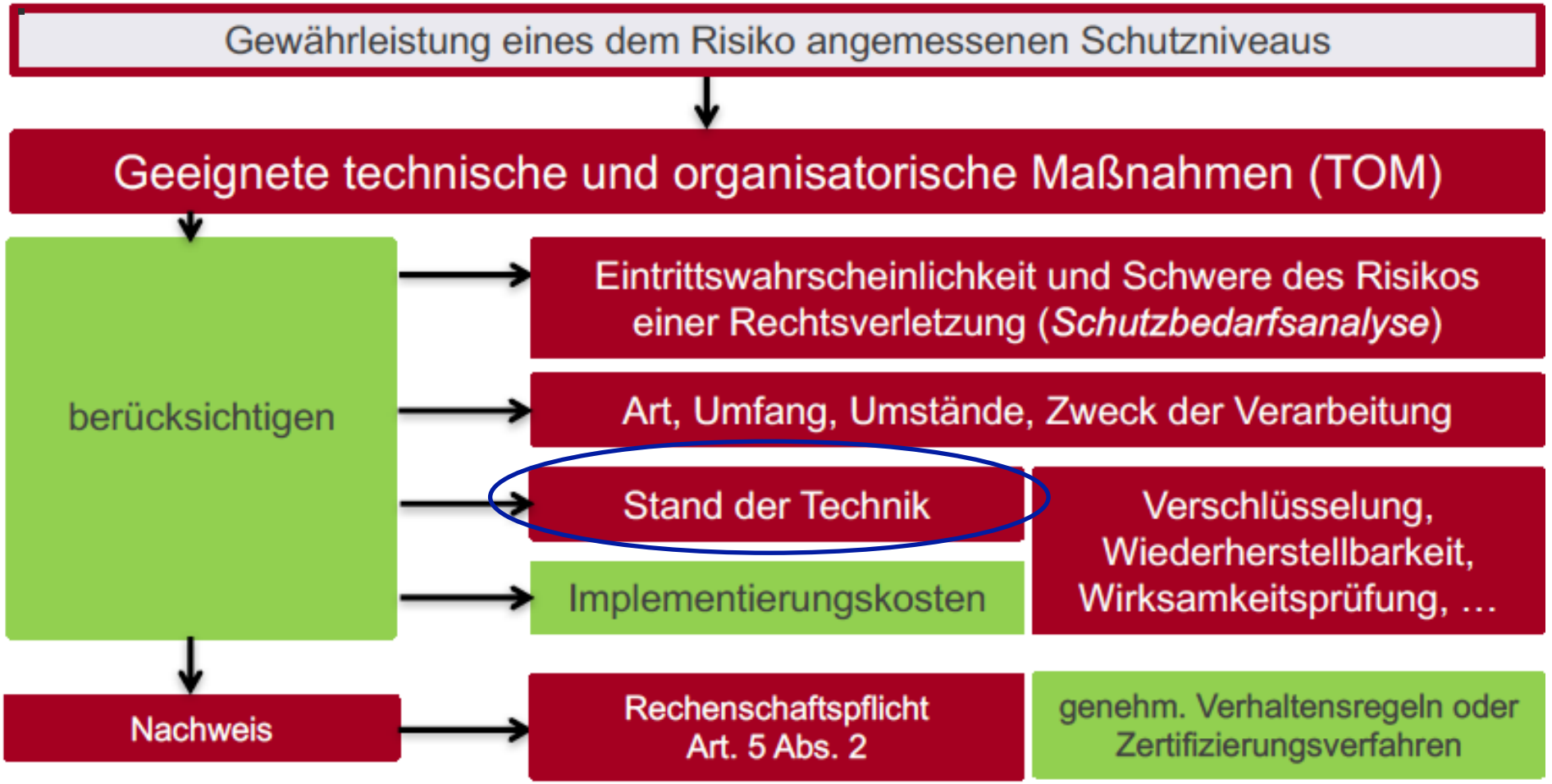
- Die Datenschutz-Grundverordnung sorgt ohnehin schon für reichlich Stress, aber eine spezielle Anforderung der DSGVO sorgt für besondere Verwirrung:
  - **Artikel 32 verpflichtet Unternehmen, ihre Daten dem „Stand der Technik“ entsprechend zu schützen.** Das Problem dabei: IT-Entscheider und Hersteller sind sich in der Interpretation dieser Vorgabe alles andere als einig.
  - Die Formulierung „Stand der Technik“ findet sich auch **in § 8a des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)** von 2015. Dieses schreibt vor, dass kritische Infrastrukturen entsprechend geschützt werden.
  - Auch in der **Anlage zum §9 BDSG** ist die Formulierung bereits zu finden. Allerdings nur auf Verschlüsselung bezogen, während sie die DSGVO auf alle Schutzmethoden ausweitet.
- Mit Artikel 32 der DSGVO wird der „Stand der Technik“ zur allgemeinen Richtschnur für den Schutz personenbezogener Daten erklärt
  - Allerdings sind sich Experten - ob Juristen oder IT-Spezialisten - im Grundsatz einig: **Präzise Formulierungen schaden mehr als sie nützen.**

Copyright © 2018 Holger Schellhaas. All rights reserved.
No part of this document may be reproduced or distributed in any form without prior written permission by Holger Schellhaas

„Stand der Technik“ nach DSGVO

Transformation Consulting International

Sicherheit der Verarbeitung nach Artikel 32 DSGVO



Copyright © 2018 Holger Schellhaas. All rights reserved.
No part of this document may be reproduced or distributed in any form without prior written permission by Holger Schellhaas

„Stand der Technik“ nach DSGVO

Transformation Consulting International

- Die Verantwortlichen müssen durch geeignete Maßnahmen die IT-**Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit** umsetzen. Ziel ist, auf Basis von Best-Practices vorhandene Richtlinien und TOMs an die Anforderungen der EU-DSGVO anzupassen.

Stand der Technik ist ...

... der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.

Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden.

[Gesetzesbegründung zu § 8a BSIG, BT-Drucks. 18/4096, S. 26]

Copyright © 2018 Holger Schellhaas. All rights reserved.
No part of this document may be reproduced or distributed in any form without prior written permission by Holger Schellhaas

„Stand der Technik“ nach DSGVO

Transformation Consulting International

- Die Verantwortlichen müssen durch geeignete Maßnahmen die IT-**Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit** umsetzen. Ziel ist, auf Basis von Best-Practices vorhandene Richtlinien und TOMs an die Anforderungen der EU-DSGVO anzupassen.

Gegenentwurf …

Beim Stand der Technik handelt es sich um die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann.

[Bartels/ Backer/ Schramm: Der „Stand der Technik“ im IT-Sicherheitsrecht - Wirkung des Verweisungsbegriffs und Lösungsansätze zur legislativen Verwendung, Tagungsband 15. Deutscher IT-Sicherheitskongress, S. 503]

Copyright © 2018 Holger Schellhaas. All rights reserved.
No part of this document may be reproduced or distributed in any form without prior written permission by Holger Schellhaas

Transformation Consulting International

TOM-Assessment - Bewertung „Stand der Technik“ - Beispiel

Maßnahmen / TOMs	Stand der Technik		Wirksamkeit prüfen
	Objektiv-technisch	Subjektive Auswahl	
Sichere Konfiguration der mobilen Geräte zur Verhinderung einer unerwünschten Kopplung zwischen Firmennetz und Internet	Konfiguration wird von einem Mobile Device Management System entgegengenommen und verwaltet	Richtlinie zum Einsatz von Mobile Device Management-Lösungen	offen
Verschlüsselung der E-Mail selbst und des Übertragungsweges zur Vermeidung von Ausspähung oder Manipulation im Transport	TLS auf allen Transport-Wegen; zusätzlich VPN mit Prüfung der Gegenstelle je nach Schutzbedarf der übermittelten Daten; Inhaltsverschlüsselung per S/MIME oder PGP	2-Faktor-Authentisierung; Zugang nur über verschlüsselte Verbindungen (TLS und/oder VPN);	offen
Kompromittierung von Anwendungen zu verhindern aufgrund von Infrastruktur-Schwachstellen	Umsetzung der Controls A.12.6 aus ISO 27002; mindestens jährliche Whitebox-Audits basierend auf dem Standard ASVS	Vulnerability-Management eingeführt (SIEM Lösung) ; laufende Qualitätskontrollen im laufenden Betrieb	offen

Quelle: BSI IT-Grundschutz, ISO 27001; TeleTrust Handreichung zum „Stand der Technik“ im Sinne des IT-Sicherheitsgesetzes (ITSIG); Best Practice TCI (CISSP-Experte); Best Practice verinice.PARTNER (Datenschutz-Auditor)

Copyright © 2018 Holger Schellhaas. All rights reserved.
No part of this document may be reproduced or distributed in any form without prior written permission by Holger Schellhaas

Transformation Consulting International

TOM-Assessment - Bewertung „Stand der Technik“ - Folgerung

- Eine Konkretisierung der relevanten Systeme und Komponenten erfolgt nicht. Also müssen wir von der Einhaltung des Stands der Technik für die vollständige IT-Infrastruktur ausgehen. Dazu gehören alle Datenübertragungs-, Speicherungs- und Verarbeitungsmöglichkeiten.
- Die In der Praxis empfiehlt es sich, in einer detaillierten Übersicht typische TOMs nach dem Stand der Technik aus objektiver Expertensicht und aus eigenen Best-Practice-Erfahrungen zu bewerten.
- Als objektive Quelle neben den Standards BSI IT-Grundschutz und ISO 27001 eignet sich dabei aus unserer Sicht hervorragend die TeleTrust Handreichung zum „Stand der Technik“ im Sinne des IT-Sicherheitsgesetzes.
- Bei der Auswahl angemessener Schutzmaßnahmen, die dem "Stand der Technik" entsprechen, sind aber immer auch wirtschaftliche Aspekte zu berücksichtigen. Ob eine Maßnahme wirtschaftlich ist, kann allerdings nur durch individuelle Betrachtung des konkreten Schutzbedarfes festgestellt werden.

Copyright © 2018 Holger Schellhaas. All rights reserved.
No part of this document may be reproduced or distributed in any form without prior written permission by Holger Schellhaas

„Stand der Technik“ nach DSGVO

Vielen Dank für die Aufmerksamkeit

Holger Schellhaas
Partner der TCI GmbH

Interim-CISO der Haspa Direkt

Schmaedelstr. 20
81245 München

mobile +49 (0) 170 240 85 70
holger.schellhaas
@tci-partners.com

Copyright © 2018 Holger Schellhaas. All rights reserved.
No part of this document may be reproduced or distributed in any form without prior written permission by Holger Schellhaas