IT-Sicherheitsrechtstag 2017

Gemeinsame Veranstaltung von TeleTrusT und BvD

Berlin, 07.11.2017

EU-Datenschutzgrundverordnung - Überblick über die operative Umsetzung bei enercity -

Thomas H. Dorstewitz

enercity

IT-Sicherheitsrechtstag 2017

Gemeinsame Veranstaltung von TeleTrusT und BvD

Berlin, 07.11.2017

EU-Datenschutzgrundverordnung

- Überblick über die operative Umsetzung bei enercity -

Thomas H. Dorstewitz - enercity

+ + + es gilt das gesprochene Wort! + + +


BusinessContinuityManagement
Künstliche-Intelligenz
Mensch-Computer-Interaktion
Kontextsensitivität
Aktoren
Informationssicherheit
CloudComputing
PervasiveComputing
MobileComputing
Public-Cloud
OLEDs
ActivityTracker
Hybrid
InternetofThings
Virtual
PC-Ära
Vernetzung
LCDs
Elektrolumineszenz-Folie
Ambient-Intelligence
EU-Datenschutzgrundverordnung
OrganicComputing
IT-Compliancemanagement
Bewegungsprofile
WearableComputing
UbiquitousComputing
Ubiquitous-Ära
Mainframe-Ära
PDA
WIMP-Interfaces
Sensoren
SmartWatches
Datenschutz
Mobile-Code
PaaS
SaaS
IaaS
TAUCIS
SmartHome
KDD
Community
RFID
IoT
IdD
LTE
Middleware
Machine2Machine
Ad-hoc-Net
ZigBee
Ethernet
UMTS
HSPA+
LEDs
Protocols
SoftwareEngineering


Technische Richtlinien
IT-Sicherheitskatalog § 11 Abs. 1a EnWG
Messstellenbetriebsgesetz
BSI Standard 100-1
BSI Grundschutz
Prozessdatenverarbeitung
Datenschutzanpassungs- und Umsetzungsgesetz
IT-Sicherheit
BSI Standard 100-4
Mapping
BSI Standard 100-2
ISO/IEC 27002
Informationssicherheit
ISO/IEC TR 27019
IT-Sicherheitsgesetz
BSI Kontaktstelle und -Meldeprozess
BSI Standard 100-3
BDEW Whitepaper
IT-Sicherheitskatalog § 11 Abs. 1b EnWG
EU-Datenschutzgrundverordnung
Energiewirtschaftsgesetz
Schutzprofile (CC-PP)
BSI TR 3109-x
ISO/IEC 27001

EU-Datenschutzgrundverordnung

enercity
positive energie

Mai 2016 – Verabschiedung EU DSGVO …

Ab 25.05.2018 gilt in der Europäischen Union einheitlich die:

- EU-Datenschutzgrundverordnung (99 Artikel)

… und zusätzlich (*1) in Deutschland das…

- Datenschutzanpassungs- und Umsetzungsgesetz (quasi das neue Bundesdatenschutzgesetz mit über 70 Paragrafen)

(*1) - zusätzlich ist auf EU-Ebene die E-Privacy-Verordnung zu erwarten
(Ersatz für: E-Privacy-Richtlinie und Richtlinie 2009/136 (Cookie-Richtlinie))

Nebenschauplätze mit Relevanz

IT-Sicherheitsgesetz (Juli 2015)

- BSI-Gesetz (kritische Infrastrukturen)
  - ✓ Technische / organisatorische Vorkehrungen

- Energiewirtschaftsgesetz (IT-Sicherheitskatalog)
  - ✓ Etablierung eines ISMS nach ISO/IEC 27001

Gesetz zur Digitalisierung der Energiewende (August 2016)

- Messstellenbetriebsgesetz
  - ✓ Technische Richtlinien (BSI 3109-x)
  - ✓ Etablierung ISMS ISO/IEC 27001 (GWA)
  - ✓ hochgradig datenschutzrelevant

…wenn ich nicht mehr weiter weiß, bilde ich einen Arbeitskreis …

Vorgehensweise enercity

Informationssicherheitsmanagement

enercity: Bildung mehrerer Arbeitsgruppen:

- IS – Architektur der Informationssicherheit
- ISMS – Scope Netzbetrieb (S, G, W)
- ISMS – Scope Wasser (Produktion)
- ISMS – Scope Aggregatoren
- ISMS – Scope KW-Linden
- DSGVO

… gemeinsame Leitung aller Arbeitsgruppen!

Informationssicherheitsmanagement

Strategisches Ziel:

Ganzheitliches Informationssicherheitsmanagement(1)
… mit den Managementbereichen:

- Informationssicherheitsmanagementsystem (ISMS)
- Datenschutzmanagementsystem (DSMS)
- IT-Compliancemanagementsystem (IT-CMS)
- Business-Continuity-Managementsystem (BCMS)

- … denn diese Managementbereiche greifen "untrennbar" ineinander!

(1) - Siehe enercity Architektur der Informationssicherheit

Informationssicherheitsmanagement

enercity
positive energie

Vollständige Integration des (künftigen) Datenschutzmanagements in das zentrale Informationssicherheitsmanagement

- Einheitliche Informationssicherheitspolitik
- Zentrales IS-Portal (Steuerung)
- Ganzheitliche IS-Dokumente (zum Beispiel: Rollen, Audits, etc.)
- Zentrale Prozesse & Maßnahmen (1)
- Dezentrale Prozesse & Maßnahmen
- Zentrale Vorgabe wesentlicher Hilfen (Checklisten, Templates, etc.)

(1) – Beispiele: Dokumentenlenkung, Audits, IS-Risikomanagement, Datenschutzkernprozesse

EU-Datenschutzgrundverordnung Arbeitsgruppe

- Bildung Arbeitsgruppe: DSGVO (06.2016)

- Kernteam:
  - Beauftragter für Informationssicherheit (Leitung)
  - Datenschutzbeauftragter
  - Betriebsrat
  - Revision
  - Personalbereich
  - Kommerzielle DV

EU-Datenschutzgrundverordnung Arbeitsgruppe

- Bildung Arbeitsgruppe: DSGVO (06.2016)

- Erweitertes Team:
  - Alle IT-Dienstleister (intern)
  - Alle operativen Fachbereiche

EU-Datenschutzgrundverordnung
Grundlegende Vorgehensweise

Arbeitspakete (AP)

- AP 01 – Datenschutzprozesse und Rechtsgrundlagen
- AP 02 – Datenschutzorganisation, Regelungen & neue Bedarfe
- AP 03 – Auftragsdatenverarbeitung
- AP 04 – Software & TOM
- AP 05 – Personalmanagement
- AP 06 – Kundenmanagement
- AP 07 – Onlinedienste

EU-Datenschutzgrundverordnung
Grundlegende Vorgehensweise

enercity
positive energie

1. Phase I [bis circa 30.06.2017]
   - Ist-Aufnahme (siehe Arbeitspakete)

2. Phase II [bis circa 30.12.2017]
   - Bewertung und Änderungsbedarfe aus der Ist-Aufnahme
   - Neue Anforderungen aus der DSGVO

3. Phase III [bis circa 30.05.2018 und danach]
   - Umsetzung der Änderungsbedarfe und der neuen Anforderungen

Datenschutzmanagementsystem Neugestaltung I

- Kernprozesse des Datenschutzes
  - Datenschutzkonforme Datenverarbeitung(1)
  - Sicherstellung der Betroffenenrechte(2)
  - Umgang mit Datenschutzverletzungen
- … darüber hinaus:
  - Meldepflichten (Aufsichtsbehörde, Betroffene)
  - Datenschutzfolgenabschätzung (siehe IS-Risikomanagement)
  - Dokumentationspflichten (Übersicht der Verarbeitungen, Nachweis der rechtmäßigen Verarbeitung, Datenpannen, etc.)
  - Datenschutzaudits
  - Technisch/organisatorische Maßnahmen

(1) - Datenschutzgrundsätze, Rechtmäßigkeit, Transparenz, Sicherheit der Verarbeitung, AV, Dokumentation

(2) - Transparente Information, Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Widerspruch, Automatisierte Entscheidungen, Widerruf Einwilligung

Datenschutzmanagementsystem Neugestaltung II

- Das (neue) Datenschutzmanagementsystem …

  - ✓ … analog ISO/IEC 27001
  - ✓ … risikoorientiert (ABC)
  - ✓ … methoden-/tool-basiert (z.B. PIA, Stand der Technik)
  - ✓ … workflowgesteuert(1)
  - ✓ … Checklisten-getrieben
  - ✓ ... zentrale Textbausteine & Templates
  - ✓ … OnePager im Onlinebereich

(1) - Berücksichtigt die beteiligten Managementsystem und die betriebliche Mitbestimmung

EU-Datenschutzgrundverordnung
Im Detail: AP 04 – Software & TOM

enercity
positive energie

Software

- Welche Software-Komponenten sind von der DSGVO betroffen?
- Welche datenschutzrechtlichen Anforderungen bestehen künftig?
- Können/werden die Software-Komponenten die DSGVO vollständig unterstützen ("Recht auf Vergessen", Datenübertragbarkeit, etc.)
- Wenn nicht, was ist technisch / organisatorisch zu tun?
- Umgang mit dem "Datenbestand" (prüfen der Zulässigkeit!?)

TOM (technische / organisatorische Maßnahmen)

- Ermitteln und Bewerten der aktuellen TOM
- Anpassungsbedarfe umsetzen (Beispiel: Anonymisieren / Verschlüsseln von (Test-) Daten

EU-Datenschutzgrundverordnung Hindernisse vor/während Umsetzung

- Datenschutz …
  - … wird oft als "störend" empfunden, ist wenig "sexy"
  - … die grundlegende Ziele (der Sinn) werden oft wenig verstanden
  - … wird nicht als Teil des Ganzen, sondern mehr als lästiges "Etwas" gesehen
  - … Datenschutzwissen ist eher rudimentär vorhanden
  - … wird oft erst nachträglich (durch Intervention) berücksichtigt
  - … kein bestehendes Datenschutzmanagementsystem

EU-Datenschutzgrundverordnung Chancen & Risiken

- Risiken
  - Die Betroffenen verlieren den "Anschluss"
  - Datenschutz-Akzeptanz sinkt weiter, weil (noch) komplexer
  - Permanenter Verstoß gegen Datenschutzregelungen?
  - Extreme Bußgeldzahlungen / Haftung der Verantwortlichen

- Chancen
  - Datenschutz neu denken
  - Aufräumen alter Baustellen
  - Strukturiertes Datenschutzmanagement – höhere Akzeptanz!?
  - Datenschutz als Wettbewerbsvorteil in einer digitalisierten Welt
  - Integration in das Informationssicherheitsmanagement

EU-Datenschutzgrundverordnung

enercity
positive energie

… alles bleibt!

… aber

ANDERS!

Vielen Dank
für Ihre Aufmerksamkeit!

Thomas H. Dorstewitz - enercity
Abteilung Unternehmenssicherheit - Geschäftsfeld Informationssicherheit

informationssicherheit@enercity.de

Backup-Folien

EU-Datenschutzgrundverordnung
Historie europäisches / nationales Recht

Artikel 12 (UN Menschenrechts-konvention - 1948)	Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.
Artikel 8 (Menschenrechts-konvention der EU - 4.11.1950/3.9.1953)	Schutz personenbezogener Daten (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. *Bestandteil des Rechts auf Achtung des Privatlebens ist auch das Recht auf informationelle Selbstbestimmung. Artikel 8 EMRK enthält damit auch eine rudimentäre Verpflichtung der Staaten zum Schutz der Daten seiner Bürger.*
Art. 16 AEUV (VERTRAG ÜBER DIE ARBEITSWEISE DER EUROPÄISCHEN UNION)	(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Das Europäische Parlament und der Rat erlassen gemäß dem ordentlichen Gesetzgebungs-verfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht.
EGMR (1959)	Etablierung des Gerichtshofes für Menschenrechte zur Durchsetzung der Verpflichtungen aus der EU Menschenrechtskonvention.

EU-Datenschutzgrundverordnung
Historie europäisches / nationales Recht

enercity
positive energie

Richtlinie 95/46/EG	**Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (Datenschutzrichtlinie)**
Richtlinie 2002/58/EG (e-Privacy-Richtlinie)	**RICHTLINIE 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)**
Bundesdatenschutz-gesetz	Bundesdatenschutzgesetz (BDSG) (1. Fassung: 1.1.1979) Novellierungen: 1991, 2001 (durch EU Datenschutzrichtlinie), 2006, 2009 Weitere spezialgesetzliche Regelungen: Telekommunikationsgesetz Telemediengesetz Gesetz über den unlauteren Wettbewerb
Art. 1 DS-GVO	Gegenstand und Ziele (1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. (2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. (3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

EU-Datenschutzgrundverordnung
Democracy – im Rausch der Daten

enercity
positive energie

… Empfehlung!

Der Dokumentationsfilm zur EU-Datenschutzgrundverordnung

Einblicke in die Entstehungsgeschichte der EU-Datenschutzgrundverordnung und den "Politikbetrieb EU"