IT-Sicherheitsrechtstag 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 14.11.2019

DSGVO und KRITIS: Umsetzung am Praxisbeispiel enercity AG

Thomas H. Dorstewitz, enercity AG

enercity
positive energie

… alles bleibt!

… aber anders!

Zur Person/Aufgabe

Stellung im Unternehmen:

- Beauftragter für Informationssicherheit (CISO)
- Sachverständiger für den Betriebsrat (gemäß § 80 BetrVG)

Definition: enercity Informationssicherheit

- IT-Compliancemanagement
- Informationssicherheitsmanagement
- Business-Continuity-Management (IT-bezogen)
- Datenschutzmanagement

Vorab: Umfeldsituation

2015-2019

Durch das sogenannte IT-Sicherheitsgesetz (BSI-Gesetz, Energiewirtschaftsgesetz) konkrete Vorgaben …

- Umsetzung IT-Sicherheitskatalog § 11 a EnWG (Netzbetrieb Strom, Gas) … damit verbunden:
  - Aufbau und Betrieb eines Informationssicherheitsmanagementsystems (ISMS) auf Basis von ISO/IEC 27001, 27002 und 27019

- Umsetzung technischer und organisatorischer Maßnahmen auf Grundlage von § 8 ff BSI-Gesetz
  - Netzbetrieb Wasser
  - Wassergewinnung
  - Aggregatoren (vKW)

Zielvorgabe: Zertifizierung des ganzheitlichen und mehrstufigen ISMS (mit mehreren Scopes) „in Time“

Vorab: Umfeldsituation

2015-2019

- Verabschiedung „EU Datenschutzgrundverordnung“ ; Wirksamkeit: 25.05.2018
- Verabschiedung „Bundesdatenschutzgesetz“; Wirksamkeit: 25.05.2018

Zielvorgabe: Erfüllen der gesetzlichen Voraussetzungen zum Datenschutz
→ damit verbunden: Betrachten der „Sünden der Vergangenheit“ und ggf. Beheben der Selbigen!

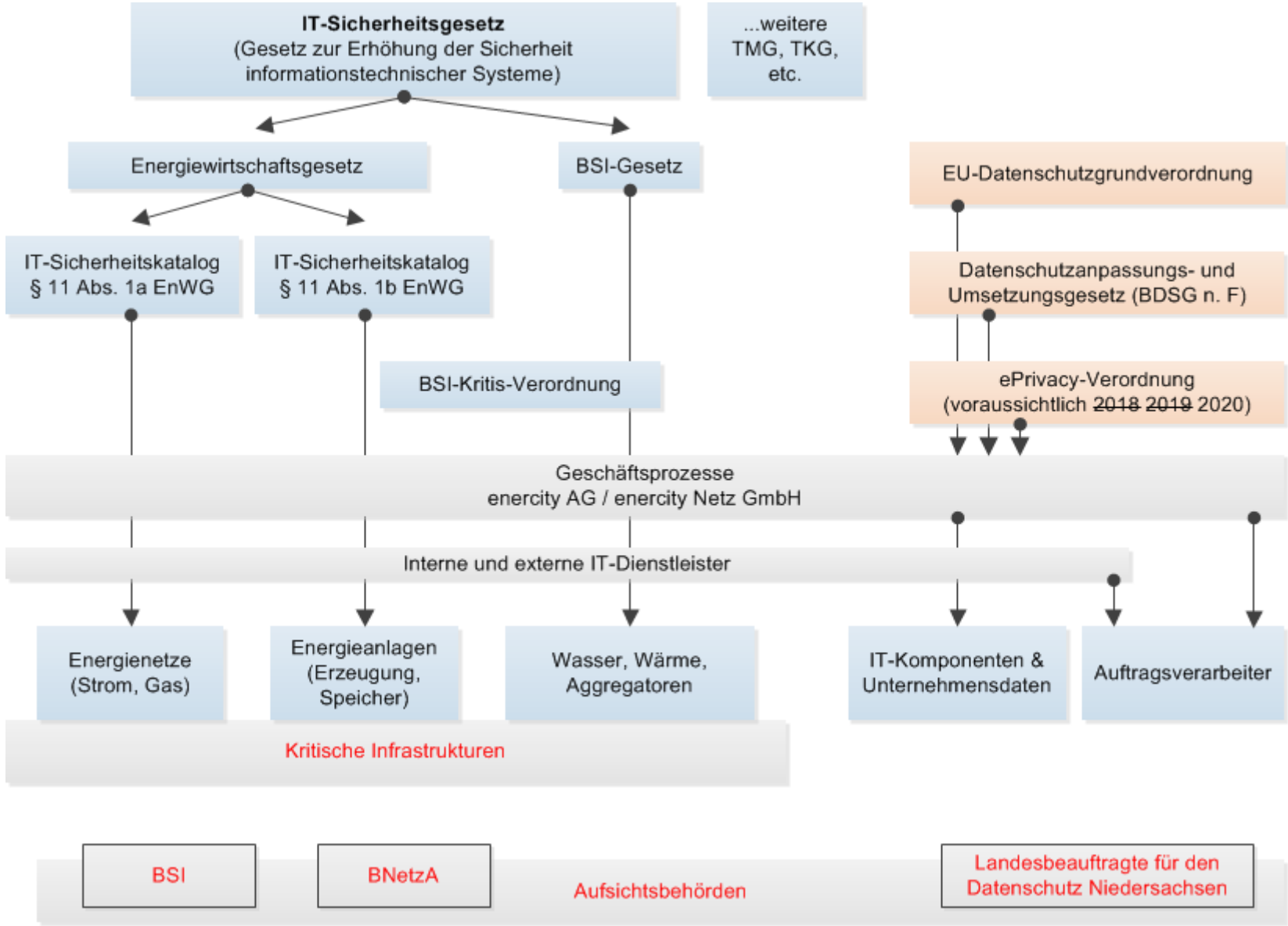
Anmerkung: Eine Projektleitung für alle Themen!
Ziel: → Informationssicherheitsmanagement als integrierte Architektur

Vorab: Umfeldsituation

…die Duplizität der Ereignisse …

oder

…wer hat sich da abgestimmt?!


IT-Sicherheitsgesetz
(Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme)
...weitere TMG, TKG, etc.
Energiewirtschaftsgesetz
BSI-Gesetz
EU-Datenschutzgrundverordnung
IT-Sicherheitskatalog § 11 Abs. 1a EnWG
IT-Sicherheitskatalog § 11 Abs. 1b EnWG
Datenschutzanpassungs- und Umsetzungsgesetz (BDSG n. F)
BSI-Kritis-Verordnung
ePrivacy-Verordnung (voraussichtlich 2018 2019 2020)
Geschäftsprozesse enercity AG / enercity Netz GmbH
Interne und externe IT-Dienstleister
Energienetze (Strom, Gas)
Energieanlagen (Erzeugung, Speicher)
Wasser, Wärme, Aggregatoren
IT-Komponenten & Unternehmensdaten
Auftragsverarbeiter
Kritische Infrastrukturen
BSI
BNetzA
Aufsichtsbehörden
Landesbeauftragte für den Datenschutz Niedersachsen

Vorgehensweise

… wenn ich nicht mehr weiter weiß …

bilde ich eine Arbeitsgruppe …

Vorgehensweise enercity

Bildung paralleler Arbeitsgruppen

2016

- IS – Architektur des (neuen) Informationssicherheitsmanagements
- ISMS – Scope Netzbetrieb (S, G)
- ISMS – Scope Netzbetrieb (W)
- EU-Datenschutzgrundverordnung (AG DSGVO)

2017

- ISMS – Scope Wassergewinnung

2019

- ISMS – Scope Aggregatoren

Anmerkung: Eine Projektleitung für alle Themen!

Ziel: → Informationssicherheitsmanagement als integrierte Architektur

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!

Erwartungshaltung Vorstand: Einhalten der gesetzlichen Vorgaben „In Time“

(1) - Siehe enercity Architektur der Informationssicherheit

Informationssicherheitsmanagement
Operative Ziele

- 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, Textbausteine, etc.)

→ Integriertes Informationssicherheitsmanagementsystem

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

Informationssicherheit Timeline

Scope	Zieldatum	Tatsächlich
IS-Architektur	2016	2016
Zertifizierung zentrales ISMS (DACH)	1. Q. 2018	01.2018
Zertifizierung ISMS Netzbetrieb (S, G)	1. Q 2018	01.2018
Zertifizierung ISMS Netzbetrieb (W)	1. Q. 2018	01.2018

Informationssicherheit Timeline

Scope	Zieldatum	Tatsächlich
Umsetzung der Anforderungen zur DSGVO / BDSG	28.05.2018	28.05.2018(1)
Zertifizierung ISMS Wassergewinnung	1. Q. 2019	02.2019
Zertifizierung ISMS Aggregatoren	4. Q 2020	
Zertifizierung Datenschutzmanagement ISO/IEC 27701	2020/2021	
(1) – Überhang diverser Restarbeiten (z. b. Methodenentwicklung)		

Informationssicherheit
Hindernisse vor/während der Umsetzung

- Neue Teilnehmer treten verstärkt auf die „Bühne“:
  - Betriebsrat, Datenschutzbeauftragter, Beauftragter für Informationssicherheit, Wirtschaftsprüfer, Banken/Versicherungen

- Die Informationssicherheit und der Datenschutz, sowie das gesamte Drumherum, rückt wesentlich stärker in den Vordergrund.

- Erwartungshaltung der Beteiligten enorm (teilweise Überforderung und Hilflosigkeit); „Betreutes Wohnen“

- Zitat eines Betroffenen nach dem Studium eines (regulatorischen) Papieres zur Informationssicherheit:

„Ich habe das Papier gelesen und nicht ein Wort davon verstanden!“

Informationssicherheit
Hindernisse vor/während der Umsetzung

- Die Beschäftigten sind allesamt gut qualifiziert und gut ausgebildet, um die Prozesse zu steuern … aber nahezu ausschließlich „elektrisch“ ausgebildet!

- Die Anforderungen an die „elektrisch“ qualifizierten Beschäftigten im PDV-Bereich steigen enorm:
  - IT-Spezialwissen (Planung, Konzeption, Betrieb, Methoden)
  - IT-Compliance (Betriebsrat, Datenschutz, IT-regulatorische Anforderungen)

- Betriebliche Mitbestimmung (§ 87, Abs. 1 Nr. 6 BetrVG)

- Die ISO/IEC 27001 selbst fordert (Abschnitt: 7.2) Personen mit entsprechenden Kompetenzen → Zielkonflikte sind vorprogrammiert! → Informatiker für PDV!?

Schwerpunkt Datenschutz

Informationssicherheit
Bemerkenswertes

Datenschutz im Speziellen …

- 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;
- DS-Wissen ist (wenn überhaupt) eher rudimentär vorhanden;
- wird oft erst nachträglich (durch Intervention) berücksichtigt;
- fehlendes Datenschutzmanagementsystem;
- Rollenverständnis: Wer ist eigentlich verantwortlich?

„Struthio-camelus-Strategie“ / Ostrich Effect“
„Ich sehe dich nicht, also siehst du mich auch nicht“

Informationssicherheit
Schwerpunkt: Datenschutz

Phase I – Ist-Aufnahme

- Aktuelle interne Verarbeitungsübersicht
- Geregelter Prozess bei Einführung neuer IT
- Bestehendes Managementsystem zur Informationssicherheit

- vorhandene Dokumentationen (ADV, etc.) nicht zentral verfügbar
- kein systematisch vorhandenes Datenschutzmanagementsystem
- Datenschutzbeauftragter zeitlich wenig verfügbar (extern)
- Verunsicherung über das WAS und WIE bei allen Beteiligten

- Die datenschutzrechtlichen Regelungen, deren Lesbarkeit und Interpretation überfordern die Beteiligten
- fehlende praktische Erfahrungen mit der DSGVO, besonders auch Extern

Informationssicherheit
Schwerpunkt: Datenschutz

enercity
positive energie

Phase II – Bewertung und Änderungsbedarfe

- Eine gewisse Aufbruchsstimmung „Datenschutz neu zu denken“
- Der Vorstand steht positiv hinter dem Projekt ☺ → BETROFFEN!
- Der gesetzliche „Druck“ motiviert alle Beteiligten

- Wenig Konkretes am Markt verfügbar
- Gerade auch die Datenschutzbeauftragten geraten unter Erwartungsdruck
- Aufsichtsbehörden müssen sich zu vielen Themen erst finden
- Alte Baustellen werden erkannt (Testdaten, Anonymisierung, Verschlüsselung, Dokumentation)
- Rollenverteilung / Rollenverständnis; wer ist eigentlich für was verantwortlich?
  → viele „Befürchtungen“ verhindern häufig konstruktives Zusammenarbeiten

Informationssicherheit
Schwerpunkt: Datenschutz

enercity
positive energie

Phase III – Umsetzung

- Vorhandenes Managementsystem zur Informationssicherheit gibt die Richtung vor
  → Erfahrungen mit Managementsystem
- Vorteile der gemeinsamen Projektleitung „All-In“ …
  → aber: es bleibt alles an IHM hängen

- Unsicherheit, ob die neue Richtung zielführend ist
- Erwartungshaltung interner Bereiche an die Projektleitung und den DSB extrem hoch und steigend!
- Eigene Verantwortungen nicht bewusst … abwartende Haltung
- Wenige „tragen“ viel, viele „tragen“ wenig
- Risikoorientierung durchgehend berücksichtigen

Informationssicherheit
Schwerpunkt: Datenschutz

Baustelle: Software-Komponenten

- 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)
  - „Stand der Technik“ – Was? Wie? Wer? → „Handreichung TeleTrusT“!! ☺
  - Ermitteln und Bewerten der aktuellen TOM
  - Anpassungsbedarfe umsetzen (Beispiel: Anonymisieren / Verschlüsseln von (Test-) Daten

Informationssicherheit
Schwerpunkt: Datenschutz

Datenschutzfolgenabschätzung

- Schutzbedarfsfeststellung der Unternehmensdaten
- Methode zur DSFA entwickeln (aktuelle Beispiele sind sehr umfangreich (ULD) → kann das tatsächlich geleistet werden?

Software-Komponenten unterstützen die datenschutzrechtlichen Anforderungen nur unzureichend.

- Recht auf Datenübertragbarkeit
- Alter Hut: Löschen von Daten

- Migration „Verzeichnis von Verarbeitungstätigkeiten“

Informationssicherheit
Schwerpunkt: Datenschutz

- Verträge zur Auftragsverarbeitung allesamt neu abschließen.
  - Welches Template darf es denn sein? Mein / Deins?
  - Zusätzliches Verzeichnis der Verarbeitungstätigkeiten, wer parallel auch Auftragsverarbeiter ist
- Gemeinsam Verantwortliche! (Beispiel: Facebook-Fan-Pages)
- Was ist eine Datenschutzverletzung?
  - Sensibilisierung aller Beteiligten! … und zwar regelmäßig
  - Man stelle sich vor, eine erhebliche „Datenpanne“ tritt ein und niemand merkt es!

Informationssicherheit
Schwerpunkt: Datenschutz

- Operationalisieren des Datenschutzmanagement

  - Dokumentationsanforderungen umsetzen (Wiki)
  - Umsetzen der beschriebenen Prozesse … nach und nach
  - Entwickeln von Tools & Checklisten (IS-Toolbox, IS-Checkbox)
  - Ausbildung von Auditoren
  - Interne Audits einplanen und Durchführen → Auditprogramm
  - Weiterentwicklung durch praktische Erfahrungen
  - Grundlegende Risikoorientierung aufbauen → IS-Risikomanagement auch für Datenschutz

- Zertifizierung des Datenschutzmanagementsystems (ISO/IEC 27701)

  - Ziel: 2020/2021 (Wunsch des Vorstands)

Informationssicherheit
Schwerpunkt: Datenschutz

- Datenschutzbewusstsein (Awareness): Die Sicherstellung der datenschutzrechtlichen Anforderungen (Datenschutz-Compliance) ist nicht allein durch technische / organisatorische Maßnahmen sicherzustellen! Es bedarf bei allen Beteiligten … :
  - … eines Bewusstseins
  - … einer Befähigung
  - … einer Bereitschaft
- Daher sind kontinuierlich durchzuführen …
  - Sensibilisierungen
  - Schulungen

Informationssicherheit
Schwerpunkt: Datenschutz

enercity
positive energie

Endlich geschafft!!!

- Am 25.05.2018 waren die (wesentlichen) Anforderungen zum Datenschutz umgesetzt und die „AG DSGVO“ formal beendet … tatsächlich ging es aber weiter!

- Ab dem 26.05.2018 gab es dann den „Aktionsplan Datenschutz 2020“
  - Weiterarbeit an „alten Baustellen“
  - Umsetzen von Nacharbeiten und weiterer Themen (z. b. Risikomanagement)
  - Weitere Operationalisierung des neu etablierten Datenschutzmanagementsystems (z. b. Prozesse, Dokumentation)

enercity
positive energie

… alles bleibt!

… aber anders!

Informationssicherheit
Schwerpunkt: Datenschutz

enercity
positive energie

… und es geht noch weiter!

Die Aufsichtsbehörde klopft an

29.06.2018

- Schreiben „Die Landesbeauftragte für den Datenschutz Niedersachsen“ (LFD); Titel:

  Einhaltung datenschutzrechtlicher Bestimmungen
  hier: Querschnittsprüfung zur Umsetzung der Datenschutzgrundverordnung

- Beantwortung eines Fragenkataloges (10 Fragen) bis zum 17. August 2018

Anmerkung: Der Eingang dieses Schreibens hat sich recht schnell herum gesprochen. Es gab zahlreiche Anfragen und alle wollten konkret wissen, was genau die LFD prüfen wird; eine gewisse „Beunruhigung“ war deutlich zu spüren! ☺

Die Fragen

1. Vorbereitung auf die DSGVO

… Schilderung der konkreten Vorbereitungen und der Durchführung zur Umsetzung

2. Verzeichnis von Verarbeitungstätigkeiten

… Darstellung des Prozesses zur Vollständigkeit und zur Aktualität. Übermittlung einer Übersicht aller Verfahren und eines konkreten Musters

3. Zulässigkeit der Verarbeitung

… Benennung der jeweiligen Rechtsgrundlagen und – soweit mit Einwilligungen gearbeitet wird – übermitteln der verwendeten Muster.

Die Fragen

4. Betroffenenrechte

… Darstellung des Prozesses zur Sicherstellung der Einhaltung, Beschreiben, wie die Informationspflichten eingehalten werden, übermitteln der verwendeten Muster.

5. Technischer Datenschutz

… Risikoorientierung der TOM, Stand der Technik, dokumentierte Rollen- und Berechtigungskonzepte, Gewährleistung Privacy by Design / by Default

6. Datenschutzfolgenabschätzung

… erkennen der Verfahren, Durchführung der DSFA, welche sind bereits erkannt und bewertet, übermitteln der Dokumentation

Die Fragen

7. Auftragsverarbeitung

… bestehende Verträge angepasst, verwendete Muster, übermitteln eines Beispielvertrages

8. Datenschutzbeauftragter

… Einbindung in die Organisation

9. Meldepflichten

… Beschreiben des Prozesses, Sicherstellung der Fristen

10. Dokumentation

… Nachweise über die Einhaltung der unter Ziffer 1. – 9. genannten Pflichten

Zeit der Betroffenheit

- Der Vorstand - als Adressat der Querschnittsprüfung - war bereits während des DSGVO-Projektes hoch sensibilisiert; dennoch neue „Betroffenheit“ auf allen Ebenen

- Im Vorfeld gab es zahlreiche interne Anfragen, was denn konkret gefragt und nachgewiesen werden muss (hohe Verunsicherung)

- Das laufende Projekt zur DSGVO hat sicherlich diese besondere Sensibilität mit begründet

Anmerkung: Erschwerend kam hinzu, dass der Vorstand das gesamte Unternehmen vollständig neu strukturiert und wir mitten in der Umsetzungsphase waren.

Zeit der Beantwortung

- Die Beantwortung der Fragen erschien zunächst deutlich; bei der Bearbeitung kamen jedoch zahlreiche Gedanken/Fragen:
  - Was genau ist wohl gemeint?
  - Wie detailliert ist zu antworten?

Anmerkung: Es wäre hilfreich gewesen, zu den einzelnen Fragen, etwas mehr über die Erwartungshaltung und mögliche Bewertungskriterien zu erfahren → Kriterienkatalog

Zeit der Beantwortung

- Wir haben die Fragen – im Rahmen unserer Interpretation – vollständig, aber in der gebotenen Kürze, beantwortet
  - Antworten in Tabellenform (12 Seiten)
  - Anlagen (circa 25 Seiten)

- Hilfreich war:
  - … das wir das Thema Datenschutz auch vor der DSGVO „ernst“ genommen und aktiv gelebt haben
  - … bestehende Prozesse etabliert waren; neue kamen hinzu
  - … wir Parallelprojekte zur Informationssicherheit hatten (IS-Risikomanagement, Aufbau Managementsysteme, Dokumentation)

Zeit der Beantwortung

- Was wir (noch) nicht hatten:
  - IT-Verfahren (> 120) waren nicht vollständig hinsichtlich der DSFA-Relevanz geprüft
  - Nach Prüfung der „Blacklist“ der Aufsichtsbehörden war mind. ein IT-Verfahren jedoch für eine DSFA identifiziert → „Pepper“, unser „humanoide Kollege“ ☺
  - Unsere Methode zur Vorabprüfung (Notwendigkeit einer DSFA) und zur Durchführung von DSFA war noch nicht vollständig fertiggestellt

Anmerkung: Nach Fertigstellung der Methode und des Tools (Excel) wurde die DSFA zu „Pepper“ nachgeliefert; vor Ort mit der LFD inhaltlich erörtert.

Abgabe und Auswertung

- Die Beantwortung aller Fragen und die geforderten Nachweise wurden fristgerecht am 16.08.2018 (Vorgabe LFD: 17.08.2018), an die Aufsichtsbehörde übergeben; „Öffentlichkeitswirksam“ im Rahmen eines GDD-Erfa-Kreises in Hannover ☺

„Der Moment der Wahrheit“

- Post von „Die Landesbeauftragte für den Datenschutz Niedersachsen“; die vollständige Auswertung unserer „Querschnittsprüfung“ wurde uns am 05.04.2019 schriftlich mitgeteilt
  - Hierbei Übermittlung des „internen“ Kriterienkataloges der LFD
  - Detailliertes Prüfergebnis zu allen Punkten des Fragenkatalogs; gute Nachvollziehbarkeit für uns

Das Ergebnis

- Die Frage aller Fragen: „Wie haben wir im Rahmen der Querschnittsprüfung abgeschnitten“

- Das Ergebnis (Zitat):

  „Nach Bewertung der einzelnen Kriterien habe ich festgestellt, dass ihr Unternehmen sich gut auf die Datenschutzgrundverordnung (DSGVO) eingestellt hat. Das Ergebnis war insgesamt sehr positiv.“

- Anmerkung: Erste Sofortmaßnahme: Kopie des Schreibens an den Vorstand der enercity AG ☺

Aktuelles & Ausblick

Unsere aktuellen Themen rund um das Datenschutzmanagement

- Ausrichten Datenschutzmanagement; ISO/IEC 27701; ggf. Zertifizierung
- Generisches Löschkonzept; DIN 66398
- Weiterentwicklung unserer „Toolbox“ zum Datenschutz (Bewertung „Datenpannen“, DSFA, Kategorisierung von Projekten, Risikomanagement, Auftragsverarbeitungen, etc.)
- Weiterentwicklung unserer „Checkbox“ (Auditmanagement-Checklisten)
- Weiterentwicklung unserer technischen und organisatorischen Maßnahmen (Stand der Technik)
  - Ganz aktuell: Zusammenarbeit mit der Aufsichtsbehörde; prüfen der Erprobungsfassung „ZAWAS“ der LFD Niedersachen

ZAWAS: Prozess zur Auswahl angemessener Sicherungsmaßnahmen (Version: 1.0), Download

Vielen Dank
für Ihre Aufmerksamkeit!

enercity
positive energie

enercity – Informations-sicherheit
Ich bin dabei!

Fragen?