IT-Sicherheit unter der Datenschutz-Grundverordnung

Sicherheitsmanagement als Compliance-Baustein

20.09.2018

Dr. Korbinian Hartl

Bezpečnost v IT a GDPR

Management bezpečnosti v rámci souladu se zákony a předpisy

Alicante
Berlin
Bratislava
Brüssel
Budapest
Bukarest
Dresden
Düsseldorf
Frankfurt/M.
Hamburg
London
Moskau
München
New York
Prag
Warschau

noerr.com

Noerr

Compliance als Schlagwort
Soulad se zákony a předpisy jako klíčová slova

Compliance – Rechtstreue und Risikovermeidung
Soulad se zákony a předpisy a vyvarování s riziků

Compliance als Schlagwort:

Bedeutung:

„Einhaltung rechtlicher Vorschriften“

Unternehmensperspektive: Begrenzte Zeit, Budgets etc.
daher in der Praxis:

„Vermeidung von Haftungs-Risiken die aus der Nichtberücksichtigung gesetzlicher Vorgaben resultieren“

DSGVO: **Schafft hohe Haftungsrisiken (insb. Bußgelder)**

Positiv: Einheitlicher Rechtsrahmen

Soulad se zákony a předpisy jako klíčová slova:

Význam:

„Dodržování právních předpisů.“

Perspektiva podniků: Omezený čas, rozpočet etc.,
proto v praxi:

„Vyhnutí se odpovědnostním rizikům vyplývajícím z nedodržení zákonných požadavků“

GDPR: ***Vytváří vysoká odpovědnostní rizika (zejména peněžní pokuty)***

Positivum: jednotný právní rámec

Noerr

IT-Sicherheit: Anforderungen der DSGVO
IT bezpečnost: požadavky GDPR

Rechenschaft : Dokumentation als Compliance-Baustein

Účetnictví: dokumentace v rámci souladu se zákony a předpisy

„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“ (Art. 5 Abs. 1 lit. A)
„zákonnost, korektnost a transparentnost“ (čl. 5 odst. 1 pís. a)

„Zweckbindung“ (Art. 5 Abs. 1 lit. b)
„účelové omezení“ (čl. 5 odst. 1 pís. b)

„Datenminimierung“ (Art. 5 Abs. 1 lit. c)
„minimalizace údajů“ (čl. 5 odst. 1 pís. c)

„Richtigkeit“ (Art. 5 Abs. 1 lit. d)
„přesnost“ (čl. 5 odst. 1 pís. d)

„Speicherbegrenzung“ (Art. 5 Abs. 1 lit. e)
„omezení uložení“ (čl. 5 odst. 1 pís. e)

„Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f)
„integrita a důvěrnost“ (čl. 5 odst. 1 pís. f)

„Rechenschaftspflicht“ (Art. 5 Abs. 2)
„odpovědnost“ (čl. 5 odst. 2)

Noerr

Art. 32 DSGVO: Geeignete **technische und organisatorische Maßnahmen**
*Čl. 32 GDPR: vhodná **technická a organizační opatření***

1

Stand der Technik

Stav techniky

2

Kosten der Implementierung

Náklady na provedení

3

Art, Umfang, Umstände und Zwecke der Verarbeitung

Povaha, rozsah, kontext a účely zpracování

4

Wahrscheinlichkeit und Schwere des Risikos

Pravděpodobnost a různá závažnost rizik

Noerr

Risikobasierter Ansatz
Přístup založený na riziku

„Wahrscheinlichkeit und Schwere des Risikos“

- Keine Legaldefinition des Begriffs Risiko
- Übliche Formel: **Risiko**:

  [Höhe des Risikos für Rechte und Freiheiten natürlicher Personen] = [Eintrittswahrscheinlichkeit einer Bedrohung] x [Schadenspotential]

- Gesetzliche Leitlinien? - Abstrakt und offen
- **Unternehmer als Risiko-Manager für den Betroffenen**

„Pravděpodobnost a různá závažnost rizik “

- *Žádná legální definice pojmu „riziko“*
- *Běžná rovnice: **riziko**:*

  [Výše rizika pro právní a fyzické osoby] = [Vstupní pravděpodobnost hrozby] x [potenciál škody]

- *Zákonné pokyny? - Abstraktní a otevřené*
- ***Podnikatel jako rizikový manažer pro dotčené osoby***

Noerr

Identifizierung und Bewertung von Risiken
Identifikace a zhodnocení rizik

Tätigkeiten mit hohem „Schadenspotential“:

- Profilbildung / systematische Überwachung
- Großer Umfang der Verarbeitung
- Automatisierte Entscheidungsfindung
- Schutzbedürftiger Personenkreis

Činnosti s vysokým „potenciálem škody“:

- *Profilování/ systematický dohled*
- *Velký rozsah zpracování*
- *Automatizované rozhodování*
- *Zranitelná skupina lidí*

„Was kann passieren?“

„Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten“

„Co se může stát?“

„Zničení, ztráta nebo změna, neúmyslná nebo nezákonná, nebo neoprávněné zveřejnění respektive neoprávněný přístup k osobním datům“

Noerr

Verhältnismäßigkeit (Aufwand : Nutzen)
Přiměřenost (náklady: užitek)

Verhältnismäßigkeit

- keine absolute Bestimmung (z.B. keine numerische Abgrenzung)
- stattdessen relativer Ansatz: Einzelfallabwägung unter Berücksichtigung aller relevanten Umstände
- Stand der Technik als ein wesentliches Kriterium
- Implementierungskosten
  - wirtschaftliche Zumutbarkeit

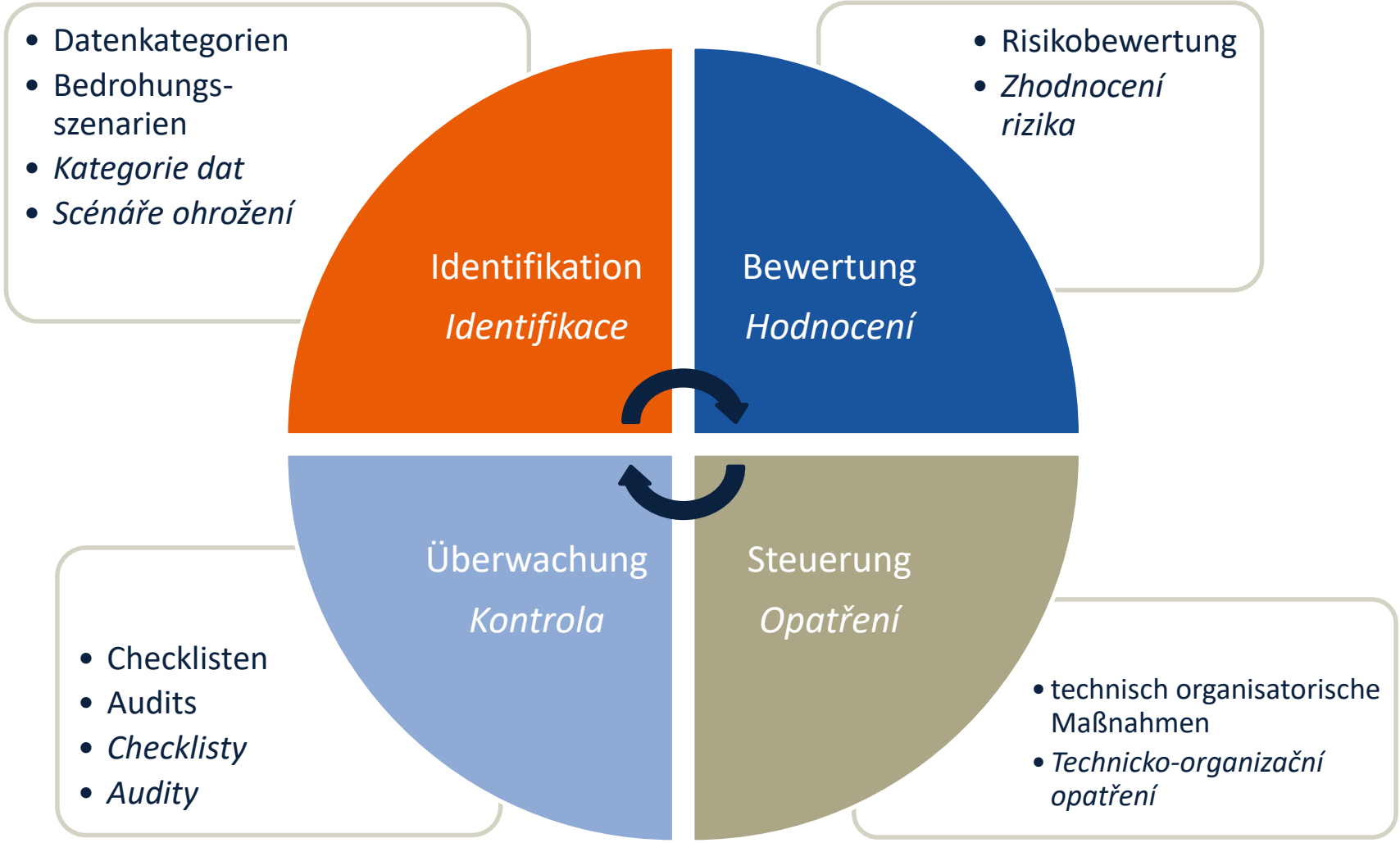
Přiměřenost

- *Žádné absolutní určení (např. žádné numerické ohraničení)*
- *Místo toho relativní přístup: individuální posouzení s ohledem na všechny relevantní okolnosti*
- *Stav techniky jako zásadní kritérium*
- *Náklady na provedení*
  - *Ekonomicky únosné*

Noerr

Umsetzung im Unternehmen
Implementace v podnikání

Implementierung der Anforderungen
Implementace požadavků



Umsetzungsmethodik – Organisatorische Voraussetzungen
Metodika implementace – organizační předpoklady

Lokalisierung von Verantwortung

- Einbindung des leitenden Managements
- Richtlinien zur operativen Verantwortlichkeit
- Ziel: „Rechenschaftsfähigkeit“

Lokalizace odpovědnosti

- *Zapojení top managementu*
- *Směrnice/předpisy k operativní odpovědnosti*
- *Cíl: „Odpovědnost“*

Einheitliche Technik der Risikobewertung + einheitliche Ablauforganisation

- Dokumentiert
- Nachvollziehbar
- Ziel: „Rechenschaftsfähigkeit“ der Bewertung und Organisation

Jednotná technika hodnocení rizika + jednotná organizace procesu

- *zdokumentováno*
- *srozumitelně*
- *Cíl: „ Odpovědnost“ hodnocení a organizace*

Anlehnung an IT-Sicherheitsstandard

Podpora IT bezpečnostního standardu

Noerr

Methodik: Ermittlung / Evaluation / Entwurf
Postup: určení/ evaluace / koncept

- Der Unternehmer als Risiko-Manager
  - Unbestimmte Rechtsbegriffe
  - Im Zweifel: Vorsichtige Bewertung

- *Podnikatel jako rizikový manažer*
  - *Nepřesné právní pojmy*
  - *Na pochybách: opatrné hodnocení*

- Ermittlung des Risikopotentials der konkreten Verarbeitungstätigkeit
- *Určení potenciálu rizika konkrétní činnosti zpracování*

- Ermittlung des Schutzbedarfes personenbezogener Daten
- *Určení požadavků na ochranu osobních dat*

- Erstellung eines Datenschutzkonzept
- *Vypracování konceptu na ochranu dat*

Noerr

Bewältigung von Risiken
Zvládnutí rizik

Allgemein: Risiken können

- vermieden (Beendigung der Datenverarbeitung)
- transferiert (Übertragung an Dritte)
- akzeptiert
- oder **minimiert** werden

- Art. 32 Abs. 1 DSGVO setzt auf **Minimierung; exemplarisch:**
  - Verschlüsselung
  - Verfügbarkeit / Vertraulichkeit/ Belastbarkeit und Integrität
  - Recovery

erneut: Rechenschaftsfähigkeit durch Dokumentation

Obecně: rizika mohou být

- *vyloučena (ukončení zpracování dat)*
- *transferována (přenesena na třetí osobu)*
- *akceptována*
- ***minimalizována***

- *Čl. 32 odst. 1 GDPR odkazuje na **minimalizaci, exemplárně:***
  - *šifrování*
  - *dostupnost / důvěrnost / odolnost a integrita*
  - *Recovery*

***opět:** odpovědnost prostřednictvím dokumentace*

Noerr

Verarbeitungsverzeichnis
Záznamy o činnostech zpracování

- Verarbeitungsverzeichnis, Art. 30 DS-GVO
  - Verzeichnis sämtlicher Verarbeitungstätigkeiten
- Ausgangspunkt des Compliance-Managements
  - Identifikation und Bewertung von Risiken anhand der Dokumentation

- *Záznamy o činnostech zpracování, čl. 30 GDPR*
  - *Správce vede záznamy o činnostech zpracování, za něž odpovídá*
- *Výchozí bod managementu v souladu se zákony a předpisy*
  - *Identifikace a zhodnocení rizik na základě dokumentace*

Verarbeitungsverzeichnis als „Accountability-Backbone“

Záznamy o činnostech zpracování jako „Accountability-Backbone“

Noerr

Vielen Dank.

Děkuji.