DATENSCHUTZ-AUDITS: EINE EINFÜHRUNG

Mag. Markus Kastelitz, LL.M. (IT-Recht)

Senior Researcher | Senior Consultant
markus.kastelitz@researchinstitute.at

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte

Web: https://www.researchinstitute.at

Mag. Lothar Gamper

Jurist
lothar.gamper@uibk.ac.at

Zentraler Rechtsdienst
Universität Innsbruck

https://uibk.ac.at/zentraler-rechtsdienst

Mag. Markus Kastelitz, LL.M., CIPP/E

- Jurist mit IT-Rechts-Ausbildung
- Zertifizierter Information Privacy Professional (IAPP)
- **Senior Researcher** und **Senior Consultant**, Research Institute – Zentrum für digitale Menschenrechte
- (Mit-)Autor datenschutzrechtlicher Publikationen
- Co-Gründer und Vorstandsmitglied **Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at**
- **Erfahrungen** in:
  - Wissenschaft (Uni Hannover, Lehrstuhl Prof. Dr. Forgó)
  - Legal Counsel (u.a. MedUni Wien, Industriekonzern, Parlamentsdirektion, RTR)
  - Datenschutzbeauftragter (MedUni Wien, Research Institute)
- **Forschungsschwerpunkte**:
  - Umsetzung der DSGVO
  - Datenschutz in der Forschung mit Schwerpunkt medizinische Forschung
  - Gesundheitsdatenschutz
  - Moderne Technologien und Datenschutz

universität innsbruck

MAG. LOTHAR GAMPER

- Jurist mit Schwerpunkten Datenschutz, Urheberrecht
- langjähriger Datenschutzbeauftragter (Universität Innsbruck, externer Unternehmens-DSB)
- Unternehmensberatung Datenschutz-Compliance (Pitagora Informationsmanagement GmbH, Innsbruck und Wien)
- Versch. Publikationen zu Datenschutz
- **Erfahrungen** in:
  - Wissenschaft (Universität Innsbruck, Prof. Hummer, u.a. Datenschutz im Europarecht)
  - Datenschutz in der Hochschullehre
- **Forschungsschwerpunkte**:
  - Datenschutz in der Forschung
  - Datenschutzrechtliche Fragen in Forschungsprojekten, aktuell zB zu Geodaten in der Energieraumplanung

AUDIT: WAS IST DAS?

- **Definition Audit** (ISO 9000, ISO 19011:2018):

„systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit Auditkriterien erfüllt sind“

→ **Ein Audit dient demnach der Ermittlung von Abweichungen des IST-Zustandes vom SOLL-Zustand.** Es soll damit systematisch festgestellt werden, ob Defizite („Delta“) bestehen und diese in der Folge beseitigt werden.

INTERNE VS. EXTERNE AUDITS

Kategorien	Interne Audits	Externe Audits	
Englische Bezeichnung	**First-Party-Audit**	**Second-Party-Audit**	**Third-Party-Audit**
Weitere Bezeichnungen	Internes Audit	Lieferantenaudit (tlw auch Kundenaudit genannt)	Zertifizierungsaudit
Beteiligte/ Durchführende	(externer) DSBA mit anderen Mitarbeitern (des Verantwortlichen; eventuell mit fachlicher Unterstützung Dritter)	Kunde und Zulieferer (eventuell mit fachlicher Unterstützung Dritter);	Externe, akkreditierte Zertifizierungsstelle

DATENSCHUTZ-AUDIT: TYPEN

Abhängig vom **Ziel** des Audits kann zumindest zwischen folgenden Audittypen unterschieden werden:

- **Prozessaudit**
- **Verfahrensaudit**
- **Produktaudit**
- **Systemaudit**

DATENSCHUTZ-AUDIT: WARUM? (1)

- **Mehrere Gründe:**
  - **DSGVO:**
    - **Rechenschafts- und Nachweispflicht** des Verantwortlichen gem Art 5 Abs 2 iVm Art 24 Abs 1 DSGVO
    - Art 32 Abs 1 lit d: „Verfahren zur regelmäßigen **Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung“
    - Artikel-29-Datenschutzgruppe (WP 173): „Einführung und **Überwachung von Kontrollverfahren**, die gewährleisten, dass die Maßnahmen nicht nur auf dem Papier bestehen, sondern in der Praxis **angewandt** werden und **funktionieren** (interne oder externe Audits usw.)“
  - **Außerhalb** des Datenschutzrechts (nicht abschließend):
    - Verpflichtendes **internes Kontrollsystem** (vgl § 82 AktG; § 22 Abs 1 GmbHG; § 39 Abs 3 SE-Gesetz; § 243 Abs 1 UGB; § 9 Abs 1 VStG uam); Leitungsorgan → funktionierendes Kontroll- und Risikomanagementsystem
    - Exkurs Verwaltungsstrafrecht: **strafbefreiendes/strafminderndes** Kontrollsystem → Nachweis einer qualitätsgesicherten Organisation, die durch externe Prüfung oder durch interne Überwachung regelmäßig kontrolliert wird

DATENSCHUTZ-AUDIT: WARUM? (4)

- Datenschutz-Audits können auf aufsichtsbehördliche Überprüfungen vorbereiten (siehe zB aktuelle Bescheide der Datenschutzbehörde in Österreich)
- Die Datenschutzbehörde berücksichtigt bei behördlichen Verfahren gemäß Art. 58 DSGVO durchgeführte Audits positiv
- Dem Verantwortlichen und dem Datenschutzbeauftragten obliegt es, ihre Überwachungspflichten zu belegen (vgl. Folie 11)

DATENSCHUTZ-AUDIT: DSBA (1)

- **Überwachungsaufgaben** des/der Datenschutzbeauftragten
  - Insb. die Wirtschaft wollte weniger (externe) Meldepflichten → Ergebnis: „Verlagerung in die Unternehmen/Institutionen“, u.a.:
  - Art 39 Abs 1 lit b DSGVO:

*„b) **Überwachung der Einhaltung** dieser **Verordnung**, anderer **Datenschutzvorschriften** der Union bzw. der Mitgliedstaaten sowie der **Strategien** des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;“*

  - **„Kernaufgabe des DSBA“**: *Drewes in Simitis/Hornung/Spiecker* (Hrsg), Datenschutzrecht (2019) Art 39 Rz 16; *König* in *Knyrim* (Hrsg), DatKomm Art 39 DSGVO Rz 12 (Stand 1.12.2018, rdb.at).

DATENSCHUTZ-AUDIT: DSBA (2)

- Regelungskonzept der DSGVO:
  - **Überwachungspflicht des DSBA**: Einhaltung der datenschutzrechtlichen Anforderungen durch den Verantwortlichen bzw Auftragsverarbeiter; genaue Reichweite bislang ungeklärt

  → Beseitigung aufgedeckter datenschutzwidriger Zustände ist davon jedoch **nicht** umfasst!

  - **Bericht** über die Prüfergebnisse (**Auditbericht**) an höchste Managementebene (Art 38 Abs 3 Satz 3 iVm Art 39 Abs 1 lit a) → Management muss die aufgedeckten Mängel abstellen (lassen)
  - Ex lege keine über den Bericht an die Geschäftsführung hinausgehenden Handlungspflichten

Siehe dazu ausf *Eßer/Menz/Meyer/Schrader-Kurz/Steffen*, Gutachterliche Stellungnahme zu Änderungen der Stellung des Datenschutzbeauftragten durch die Datenschutz-Grundverordnung 45 f mwN; *König* in *Knyrim*, DatKomm Art 39 DSGVO Rz 12 (Stand 1.12.2018, rdb.at); *Horn*, Die Rolle des Datenschutzbeauftragten nach der DSGVO, in *Krempelmeier/Staudinger/Weiser* (Hrsg), Datenschutzrecht nach der DSGVO – zentrale Fragestellungen (2018) 128.

DATENSCHUTZ-AUDIT: DSBA (3)

- Datenschutzbehörden beginnen derzeit, diese Überwachungspflichten zu kontrollieren
  - siehe zB Bayerisches Landesamt für Datenschutzaufsicht, Prüfung DS-GVO-Umsetzung bei kleinen und mittleren Unternehmen (Version 1.0) sowie Datenschutzstelle Liechtenstein, Fragebogen zur DSGVO-Umsetzung (Stand 13.11.2019):

3. Sind, falls Sie einen Datenschutzbeauftragten haben, die letzten (zwei) Audits des Datenschutzbeauftragten vorhanden und besitzen diese eine einheitliche Prüfmethodik?
   - ☐ Ja. Bitte senden Sie uns Kopien der Prüfberichte zu.
   - ☐ Nein. Grund:_____
   - ☐ Wir haben keinen Datenschutzbeauftragten.

12. → Sind,·falls·Sie·einen·Datenschutzbeauftragten·benannt·haben,·die·Prüfberichte·der·letzten·(zwei)·Audits·des·Datenschutzbeauftragten·vorhanden·und·besitzen·diese·eine·einheitliche·Prüfmethodik?¶

☐ → Ja.·Übermitteln·Sie·Kopien·der·Prüfberichte!¶

☐ → Nein.·Grund:·Klicken·Sie·hier,·um·Text·einzugeben.¶

DATENSCHUTZ-AUDIT: WER FÜHRT DAS DURCH?

- **Zuständigkeit für interne Audits/Überprüfungen:**

  Abgrenzungsproblem

  - Interne Revision/QM/Organisationsentwicklung

  versus

  - Datenschutzbeauftragter

- Idealfall (gibts den?): Es dürfen **nicht** jene, die die Einhaltung von internen Richtlinien und Standards **kontrollieren**, an deren Entstehung entscheidend **mitwirken** und so „sich selbst kontrollieren“

→ interne Koordination ist gefragt

DATENSCHUTZ-AUDIT: VORAUSSETZUNG

Internes Datenschutz-Audit:

- **Grundvoraussetzung** für die Ausübung der Überwachung der Datenschutz-Compliance durch den DSBA (als auch den Verantwortlichen selbst):
  - Vorhandensein auditierbarer Inhalte und Umsetzungsmaßnahmen
  - Anders ausgedrückt:

  Die Durchführung eines Datenschutz-Audits ist nur dann möglich und sinnvoll, wenn eine **ausreichende Prüfgrundlage vorhanden** ist!
  - Ansonsten bloße IST-Standerhebung → aber „besser als gar nichts“

Ablauf eines Audits

Chronologischer Ablauf	Anmerkungen
1. **Audit-Ziele** (Audit-Planung)	Festlegung der Vorgaben, die als SOLL-Zustand mit einem im Audit festzustellenden IST-Zustand abgeglichen werden (Gesetze, interne Richtlinien etc)
2. **Audit-Kriterium** (Audit-Vorbereitung)	Erstellung von Checklisten, Einbeziehung von Auditees in die Erstellung der Audit-Agenda zur Terminplanung, ggf Vorstellungs- oder Einführungsgespräche
3. **Audit-Nachweis** (Durchführung)	Sichtung von Unterlagen, Interviews, Vor-Ort-Termine etc
4. **Audit-Feststellung** (Durchführung und Nachbereitung)	Formulierung der festgestellten Abweichungen vom definierten SOLL-Zustand und den formulierten Kriterien, Empfehlungen zur Verbesserung der Compliance
5. Audit-Schlussfolgerungen (Nachbereitung)	Es ist anzustreben, dass die Geschäftsführung eines Unternehmens zu den Audit-Schlussfolgerungen Stellung nimmt und sowohl ihre eigenen darauf aufbauenden Entscheidungen dokumentiert (zB Änderung von Abläufen, Weisungen zur Behebung von festgestellten Compliance-Defiziten) als auch deren Umsetzung veranlasst und überwacht.

Weiterführende Literatur

- ***Kastelitz/Gamper*, Überwachung der Datenschutz-Compliance: Durchführung von Datenschutz-Audits durch den Datenschutzbeauftragten, in *Scheichenbauer* (Hrsg), Der Datenschutzbeauftragte (Linde Verlag 2020)**
- *Kranig/Sachs/Gierschmann*, Datenschutz-Compliance nach der DS-GVO^2 (2019) (mit Musterprüffragen aus Behördensicht)
- *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems (2014)
- *Kallmeyer/Kretschmar*, Die ISO 19011:2018, Audits erfolgreich vorbereiten und durchführen (2019; mit Vorlagendownloads)
- *Pachinger/Beham* (Hrsg), Datenschutz-Audit^2 (2017)