THE AUDIT COMPANY

„Der Datenschutz-Risiko-Prozess in der DS-GVO“

Was mein Unternehmen zur Umsetzung wissen muss

BvD-Verbandstag
am 4.5.2017

Dipl.-Ök. Stephan Rehfeld

1

THE AUDIT COMPANY

Datenschutz-Prinzipien

THE AUDIT COMPANY

Datenschutz-Prinzipien

Compliance-Sicht

- Rechtmäßigkeit der Datenverarbeitung und Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Speicherbegrenzung
- Richtigkeit
- Persönliche Teilhabe und Zugang
- Rechenschaftspflicht

Risiko-Sicht

- Integrität und Vertraulichkeit
- Verfügbarkeit (Belastbarkeit)

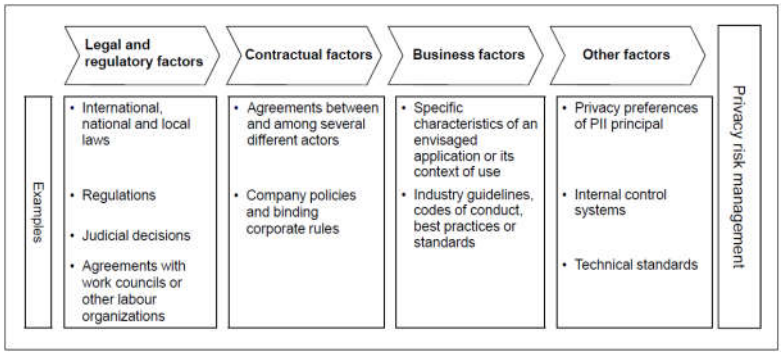
THE AUDIT COMPANY

Datenschutz-Anforderungen

(Kontext der Organisation)

THE AUDIT COMPANY

Datenschutz-Anforderungen



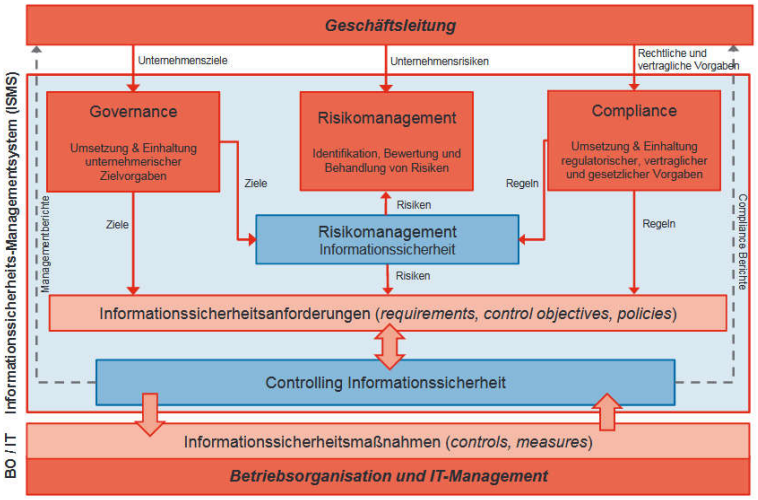
Quelle: ISO/IEC 29100:2011, Privacy Framework, S. 11

THE AUDIT COMPANY

Risikoorientierung eines Datenschutz-Managementsystems

THE AUDIT COMPANY

Einbindung des DSMS in die Unternehmenssteuerung



Quelle: ISACA, Implementierungsleitfaden ISO/IEC 27001:2013

www.dqs.de

THE AUDIT COMPANY

Auszug aus einem Datenschutz-Managementsystems

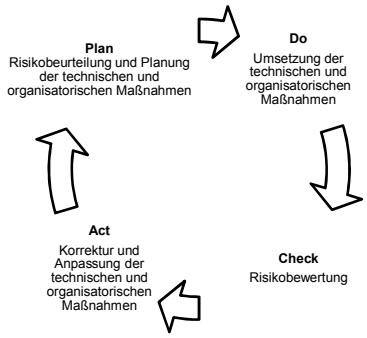
www.dqs.de

THE AUDIT COMPANY

Generelle Risikoorientierung durch Artikel 32 DS-GVO

THE AUDIT COMPANY

Risikobewertung für Vertraulichkeit, Verfügbarkeit (Belastbarkeit) und Integrität (Art. 32 DS-GVO)



THE AUDIT COMPANY

Risiko für die Freiheiten und Rechte der Betroffenen

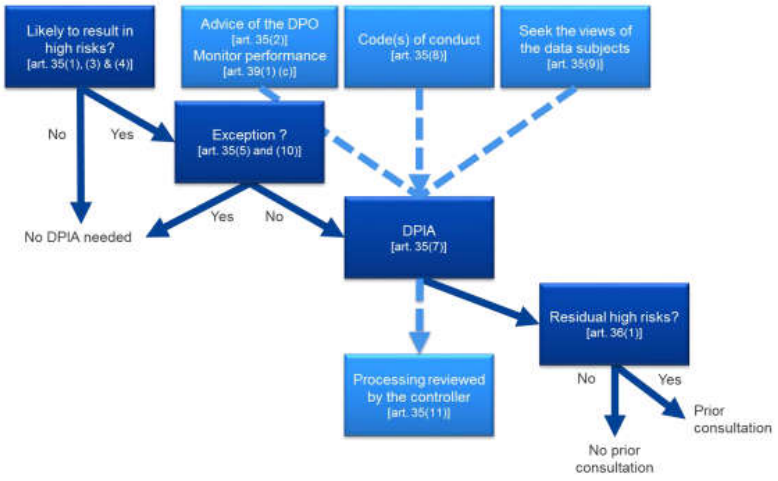
www.dqs.de

THE AUDIT COMPANY

Datenschutz-Folgenabschätzung

THE AUDIT COMPANY

Pflicht zur Durchführung eines DPIAs



Quelle: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

THE AUDIT COMPANY

Components of the DPIA (recital 90)

In risk management terms, a DPIA aims at "managing risks" to the rights and freedoms of natural persons, using the following three processes, by:

- establishing the context: "taking into account the nature, scope, context and purposes of the processing and the sources of the risk";
- assessing the risks: "assess the particular likelihood and severity of the high risk";
- treating the risks: "mitigating that risk" and "ensuring the protection of personal data", and "demonstrating compliance with this Regulation".

Quelle: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Definitionen aus der DS-GVO

- Note: the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, like it is done in certain fields (e.g. societal security), whereas risk management in some other fields (e.g. information security) is focused on the organization.
- A “risk” is a scenario describing an event and its consequences, estimated in terms of severity and likelihood.
- Article 35 refers to a likely high risk “to the rights and freedoms of individuals”.

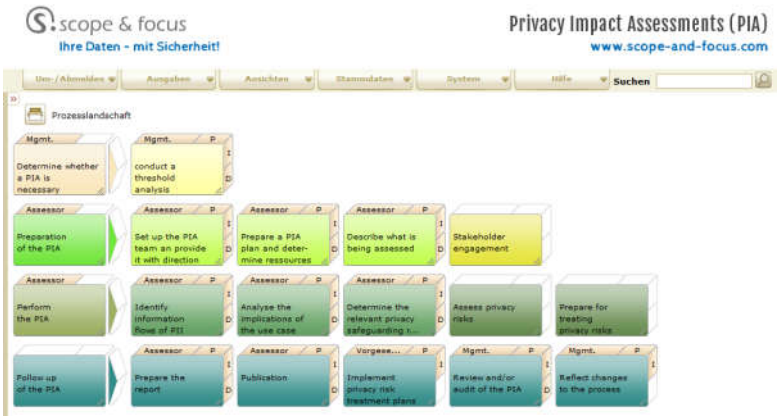
Quelle: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679

Definitionen aus der DIN ISO 31000

- Risiko (en: risk): Auswirkung von Unsicherheit auf Ziele
- ANMERKUNG 1 Eine Auswirkung stellt eine Abweichung von Erwartungen dar — in positiver und/oder negativer Hinsicht.
- ANMERKUNG 2 Die Ziele können verschiedene Aspekte umfassen (z. B. Finanzen, Gesundheit und Sicherheit sowie Umwelt) und auf verschiedenen Ebenen gelten (z. B. strategische, organisationsweite, projekt-, produkt- und prozessbezogene Ziele).
- ANMERKUNG 3 Risiken werden häufig durch Bezugnahme auf **potenzielle Ereignisse** (2.17) und **Auswirkungen** (2.18) oder eine Kombination davon charakterisiert.
- ANMERKUNG 4 Risiken werden häufig mittels der **Auswirkungen** eines Ereignisses (einschließlich von Entwicklungen) in Verbindung mit der **Wahrscheinlichkeit** (2.19) seines Eintretens beschrieben.

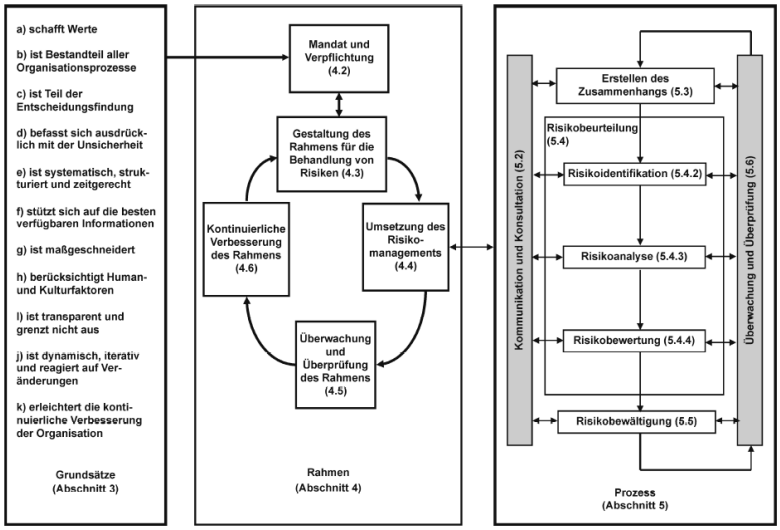
THE AUDIT COMPANY

Das Privacy Impact Assessment (PIA) am Beispiel der ISO/IEC FDIS 29134



THE AUDIT COMPANY

Risikomanagementrahmen und Risikomanagementprozess



Quelle: DIN ISO 31000:2011, Risikomanagement – Grundsätze und Leitlinien, S. 7

THE AUDIT COMPANY

Mögliche Datenschutz-Maßnahmenkataloge

THE AUDIT COMPANY

Mögliche Quelle für Informationssicherheitsmaßnahmen

8 Asset management .....
8.1 Responsibility for assets .....
8.1.1 Inventory of assets .....
8.1.2 Ownership of assets .....
8.1.3 Acceptable use of assets.....
8.1.4 Return of assets .....
8.2 Information classification .....
8.2.1 Classification of information..
8.2.2 Labelling of Information .....
8.2.3 Handling of assets .....

Quelle: ISO/IEC FDIS 29151, Code of practice for personally identifiable information protection

THE AUDIT COMPANY

Mögliche Quelle für Maßnahmen der „Organisationskontrolle“

Annex A (normative) Extended control set for PII protection..

A.1 General policies for the use and protection of PII.....

A.2 Consent and choice .....
A.2.1 Consent.....
A.2.2 Choice.....

A.3 Purpose legitimacy and specification.....
A.3.1 Purpose legitimacy.....
A.3.2 Purpose specification.....

A.4 Collection limitation.....
A.4.1 Collection limitation .....

A.5 Data minimization .....
A.5.1 Minimization .....

A.6 Use, retention and disclosure limitation .....
A.6.1 Use, retention and disclosure limitation.....
A.6.2 Secure erasure of temporary files.....

Quelle: ISO/IEC FDIS 29151, Code of practice for personally identifiable information protection

THE AUDIT COMPANY

Fachlicher Ansprechpartner und Autor:

Stephan Rehfeld
Datenschutz-Auditor

Ansprechpartnerin bei der DQS GmbH:

Antje Münzberg
Projektmanagerin Informationssicherheit
Marketing. Service. Produktmanagement.

DQS GmbH
Deutsche Gesellschaft zur Zertifizierung
von Managementsystemen

August-Schanz-Straße 21
60433 Frankfurt am Main
Tel.: +49 69 95427-0
E-Mail: info@dqs.de