www.jusletter-it.eu

Philipp E. Fischer / Ricardo Morte Ferrer

Data Protection Management System

A Useful Step Further to Protect Intellectual Capital?

Within the validity of the current data protection legislation and the proposed General Data Protection Regulation, an organization which processes personal data, has to give proof that its business processes do not affect people´s personal data in an unacceptable way. To furnish proof of this will be increasingly difficult because of the ever-increasing amount whilst collection, processing and use of personal data in the future economy. The future level of data protection in such cases will therefore increasingly depend on a more structural approach. To solve this problem, this contribution suggests the setting up of a Data Protection Management System (DPMS) based on the principles of an Information Management System (ISMS) and explained in detail by a practical example of an accurate Data Governance.

Sammlung: Tagungsband IRIS 2015
Kategorie: Beiträge
Rechtsgebiete: Datenschutz
Region: Deutschland

Zitiervorschlag: Philipp E. Fischer / Ricardo Morte Ferrer, Data Protection Management System, in: Jusletter IT 26. Februar 2015 – IRIS

Contents

1 Background

1.1 Interdependences between Data Protection and Corporate Processes

[Rz 1] Information is the most important asset in companies across the world. Anything that threatens information as the basis of IT structure directly puts the whole company's performance at risk: e.g. confidentiality, accuracy, or currency of the information or its processing functions. The early involvement of IT governance and appropriate structuring of IT processes is necessary both from an economic and a security perspective. Conversely, IT security can only be implemented effectively if all safety measures relate to clearly defined processes and service requirements. The synergy between the law and the technique should optimize processes according to these premises.

1.2 Business drivers for a Data Protection Management System

1.2.1 Personal Data, Information Lifecycle and Privacy by Design / Default principles

[Rz 2] Within the validity of data protection law and its constitutional- and European law foundations, any company which processes personal data must be able to demonstrate that its business processes do not affect people in a constitutionally unacceptable way. Thus, an increasing quantity of corporate processes depends, at every step of the information life cycle, on the handling of personal data. The aim should be easily support companies to manage data appropriately at every step of the information life cycle.

[Rz 3] An important prerequisite for the sustainable protection of personal data is the systematic

use of the principle of Privacy by Design.[1] The Commission´s proposal rightly emphasizes that companies should take, whilst collecting or processing personal data, appropriate technical and organizational measures to ensure a high level of protection of personal data. In order to support the application in as many sectors of the economy, Privacy by Design should therefore also be a mandatory criterion in the near future.

[Rz 4] Another important element of a DPMS is the sustainable protection of personal data through privacy-friendly default settings (Privacy by Default). This means, as contained in the proposal of the Commission, ensuring by appropriate settings that only data is processed according to a specific purpose.

[Rz 5] In addition, privacy-enhancing technologies (PETs), such as encryption or anonymization methods, depending on the context and the relevant risks of data processing should be made mandatory.

1.2.2 Intellectual Capital

[Rz 6] Innovative organizations are constantly faced the threat of theft of their intellectual capital. Recent announcements about the increase in industrial espionage reflect that this challenge is not being sufficiently addressed through the use of conventional methods, and that the problem is much greater than known or communicated.

[Rz 7] It is very important to differentiate between Intellectual Property (IP) and Intellectual Capital (IC)

- Intellectual Capital — An advantage or asset that is developed from the use of notable mental capacity.
- Intellectual Property — A right or possession that is developed from the use of notable mental capacity.

[Rz 8] The process to register organizational knowledge as a possession, sometimes creates the belief that the organization's knowledge is protected within this format. The truth is, these registrations are just a consolidation of some of the masses of knowledge in circulation throughout an organization

[Rz 9] Business owners are the ones who truly understand the value of the information, and the consequences of its loss. For this reason, business owners should be the protagonists of information and knowledge security, and governance of this should be built into their daily activities. Legal converts some IC into IP; IT aspires to protect everything regardless of its value

1.2.3 Conceptualization

[Rz 10] To achieve this, we need a concept for strong, coherent and effective concept. At the same time, this concept needs to create incentives for companies to invest throughout the whole life cycle on the protection of personal data, starting with the collection and processing of personal data.

[Rz 11] The concept of a DPMS could help at this point. A DPMS is based on a simple principle:

[1] Bock/Rost, Privacy by Design and the New Protection Goals — Principles, Goals, and Requirements. Retrieved March, 31st, 2013 from http://www.maroki.de/pub/privacy/BockRost_PbD_DPG_en_v1f.html.

Those who invest from the beginning in a sustainable DPMS and ensure that they keep the conditions of the mechanisms within this DPMS, will be able to benefit from the advantages of an effective implementation and enforcement architecture.

1.3 Business drivers for Data Governance

[Rz 12] Data governance, for both structured and unstructured data, is a top priority for enterprises today. Technologies like Identity Intelligence are targeted and learned by organizations who wish to tackle this important initiative. Unlike past security and risk challenges, with data governance, a «patch» solution will not do the work. The data is in-fact everywhere and a broad solution with a modular architecture is strongly needed. The discussion should begin, though, by understanding why this enterprise-wide view of the organization's data is needed. First, enterprises strive to decrease the risk of data misuse and leakage. Second, a visibility of data access from simple audit to complex ownership analysis is required. Third, business leaders need to control and monitor access privileges in a straight-forward and automatic approach (as regulatory compliance often requires them to sign and approve these privileges). In the past, these issues were considered at low priority as business leaders assumed that access controls over sensitive data are in place. Studies[2] accompanied with a rapid rise of unfortunate data misuse incidents has led executives to understand that their sensitive data is not as secured as they once believed it to be.

[Rz 13] It is clear today that a crucial part of the organization business related digital information is unstructured data. Almost a decade ago Merrill-Lynch estimated that «More than 85 percent of all business information exists as unstructured data»[3]. Now, as business leaders realize that their data is exposed and out of control, immediate actions are required:

- Audit actual data access
- Map data owners, users groups and usage patterns
- Analyze the permissions of users and groups to data
- Recommend entitlement changes to meet business and regulatory policy
- Support user permissions review & grant process

[Rz 14] Business leaders are required to gain complete ownership on their entire underlying digital data and assets. In most cases this requirement unfolds a maze of files, emails, enterprise applications records (such as ERP and CRM) — to name a few. Though these types of digital assets are different in nature their users are basically the same. For instance, a reasonable assumption on an employee from an HR department will be that he or she can access HR related folders on the NAS device, HR related collaboration sites on the enterprise portal and HR related function on the ERP application. This creates an important common ground that substantially simplifies crossing this maze. This is the reason why data governance solution must take a holistic approach that will allow business leader to gradually cover all aspects of their business rules and policy.

---

2 Johnson, Symantec Global Internet Security Threat Report, Trends for 2009, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf, last revised 12 January 2015.

3 Blumberg/Atre, The Problem with Unstructured Data, http://secs.ceas.uc.edu/~mazlack/ECE.716.Sp2010/DM.Review.Unstructured.Data/DM.Review.Discovery.1.pdf, last revised 12 January 2015.

2 Relationship between DPMS and Data Governance as part of an ISMS

2.1 Supportive and opposing principles

[Rz 15] A DPMS has to put an organization in a position to exercise a systematic planning, monitoring and support function on its own data protection compliance- and in a standardized and machine-based way. A DPMS describes a type of requirements which an Information Security Management System (ISMS) does not know. An ISMS directly protects an organization´s own interests and assets. A DPMS has, however, an additional point of view from the outset by taking into account the interests of third parties.

[Rz 16] A DPMS is firstly to meet the transparency requirements of organizations. It has to actively support the information needs of persons outside of these organizations, auditing activities of internal auditors and external supervisory authorities. In addition, a DPMS should maintain techniques that help affected persons to manage their data within organizations. And it should support infrastructures that conserve the purpose of a data processing. This aspect includes for example infrastructures that were developed as part of the (user-controlled) identity management. These techniques and infrastructures put organizations in a position to deal with secure identity attributes as well as with role pseudonyms or anonymous credentials. Last but not least a DPMS should initiate the evaluation of data protection procedures and track this progress.

[Rz 17] An ISMS defines the systematic approach to legal requirements, such as those of data protection law, only insofar as the risks of non-compliant violations are assessed from the perspective of business processes. An ISMS takes not qua infrastructure side for the rights of those affected. DPMS and ISMS are in this respect both in a mutually supportive and opposing relationship when it comes to the implementation of requirements for the processing of personal data and this difference should be stressed in the present discussion.

2.2 How to combine different approaches

[Rz 18] Nowadays there are almost no holistic DPMS´s which really earn this name. We can find some software programs and standards trying to cover these services, but their achievement is still reduced to help manage data protection compliance requirements about IT security. The ISMS Standards, like ISO 27001 or BSI Grundschutz[4] currently are possibly the best chance, because they can help organizations learning to work in a systematical way. And, not to forget, they can solve problems about IT security, and IT security is, at least, part of the whole data protection issue.

[Rz 19] A DPMS essentially supports the work of a data protection officer and intends to enable an organization to exercise a systematic planning, monitoring, intervention and support function of their own data protection compliance in a standardized and as much as possible automatized way. At this point it is important to distinguish a DPMS from an ISMS, which is already installed in most of such organizations. An ISMS directly protects the organization´s own interests and assets. It sets out the systematic treatment of legal requirements, such as those of data protection law, but only insofar as they concern the risks of a compliance violation from the perspective of business processes. An ISMS alone seems to be insufficient to solve these problems and should be

4 https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html.

supplemented by a DPMS. Because in contrast to a DPMS, an ISMS does not, qua infrastructure, care for the rights of those who are affected by the processing of personal data. DPMS and ISMS are therefore in a mutually supportive and opposing relationship to implement requirements for processes related to personal data.

[Rz 20] A DPMS has firstly to meet the transparency requirements of organizations. In relation to third parties it therefore actively supports the information needs of affected entities, the auditing activities of internal auditors and the external audit supervisors. In addition, a DPMS should include techniques that help the affected to manage their data within such organizations. And it should support infrastructures that ensure the appropriation of a data processing.

[Rz 21] A DPMS should also closely look at an ISMS as well as at other established process frameworks, such as ITIL[5], COBIT[6] or methods of quality and financial management and auditing. A prerequisite is that a DPMS can become a natural part of business processes. A DPMS has to be designed in a way to be able to check the handling of personal data in compliance with fundamental rights. Despite the content-based distance between DPMS and ISMS, a DPMS should therefore adopt best practice components of an ISMS.

[Rz 22] However, such an organizational data protection approach currently is still far from being taken into account in everyday business practice. In Germany, specialists are currently working on the establishment and certification of a measurable DPMS, e.g. the «Priventum»[7]-seal of the «datenschutz cert GmbH» and the Standard-Datenschutzmodell[8].

[Rz 23] But, compared with other organizational approaches already in place like the «IT-Grundschutz», which uses a holistic process-orientated approach to achieve an appropriate security level for all types of information of an organization, no comparable standards have so far been issued for technical-organizational data protection measures.

---

5 https://www.axelos.com/itil.

6 http://www.isaca.org/knowledge-Center/cobit/Pages/Overview.aspx.

7 Maseberg, Die datenschutz cert GmbH stellt vor: priventum — das Zertifikat für das Datenschutz-Management, in: certNews, article of 5 August 2010, https://www.datenschutz-cert.de/news/cert-news/beitrag/browse/9/bp/474/artikel/die-datenschutz-cert-gmbh-stellt-vor-priventum-das-zertifikat-fuer-das-datenschutz-management.html, last revised 12 January 2015.

8 Rost, Grundlagen des Standard-Datenschutzmodells (SDM), mit Anwendung auf BigData, https://www.datenschutzzentrum.de/sommerakademie/2013/IB10-Rost_SDM.pdf, last revised 12 January 2015.

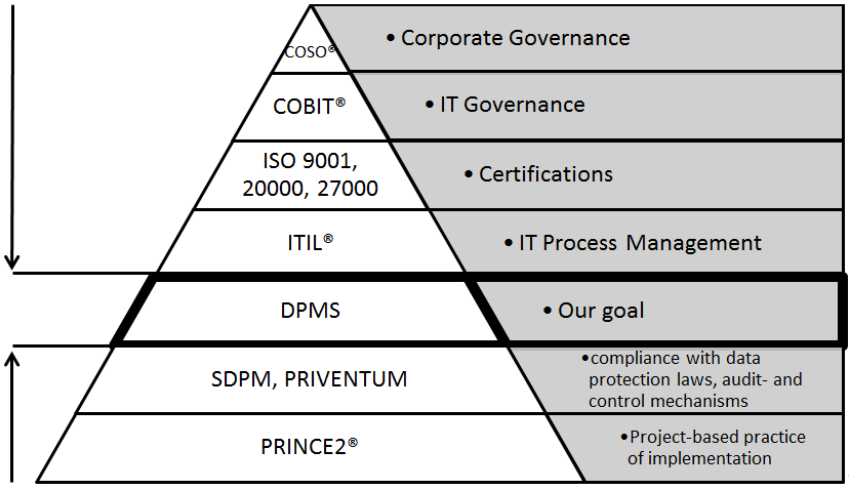


Abbildung 1: This graph illustrates the synergy of existing best practices.

3 Achieving conformance with laws, guidelines and principles

[Rz 24] Through an appropriate DPMS, several goals of Data Governance can meet requirements set out in the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)[9] and take into account international guidelines and principles, which have a great impact on the effectiveness of a DPMS:

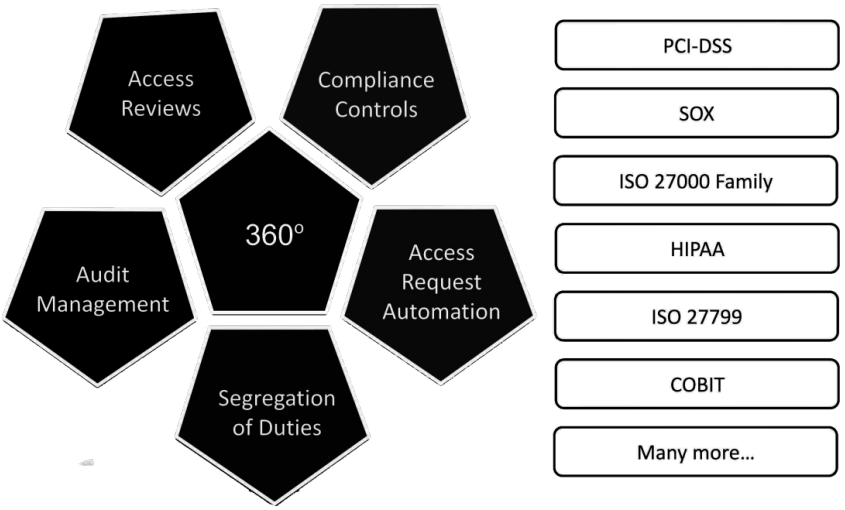
3.1 German Data Protection Law (BDSG)

Goals	BDSG
Real-time Access Control	Ensure only authorized access to the systems where personal data is stored, processed or used (access control).
Governance	Ensure that proper access control to personal data is enforced during storage, processing, access or use (create, read, update, delete).
Security	Ensure that data is protected while «in motion» and being transmitted and cannot be viewed, changed or deleted without proper authorization.
360 Degree Forensics	Ensure that you have the ability to establish and verify when and by whom personal data was entered into a computer system, as well as when and by whom this data was updated or removed.

[9] http://www.gesetze-im-internet.de/englisch_bdsg/index.html.

Audit efficiency	Ensure and have audit trails to verify that personal data is Secured, stored, processed and transmitted in accordance with the instructions and approval of the principal (individual or entity referenced in the data).
Safe keeping	Ensure that personal data is protected against accidental destruction or loss (availability control)
Integrity	Processes to ensure the integrity of employees is protected
Access Management	Ensure user information is removed from Access systems when no longer valid

3.2 International laws, guidelines and principles



10

4 Example: Whitebox Security's WhiteOPS™ Data Governance[11]

[Rz 25] In the following we aim to underline the above mentioned findings on DPMS and Data Governance through a practical example, which should highlight the lessons learnt from experiences in the field of data protection consulting.

[Rz 26] Business-wise we cooperate with Whitebox Security, a leader in the field of Identity Intelli-

10 Whitebox Security 2012, «WhiteOPs_Compliance overview».

11 Based on: Waters, Whitepaper, Unstructured Data Governance, Holistic approach to key challenges, 2012.

gence. WHitebox Security provides an industry first purpose built identity intelligence platform. With the WhiteOPS™ suite, Whitebox Security has taken a technological leap to enable, alongside with the core components of IAM Intelligence, activity monitoring, role lifecycle management and policy compliance for business activities in real-time. Whitebox Security is a solution provider for retail, financial, government and telecom.

4.1 Define Unstructured Data

[Rz 27] Unstructured data is everything we store in files: documents, spreadsheets, video, voice and images. It is spread across files servers, NAS (Network attached storage) devices, application servers and even organizational portals (like Microsoft® SharePoint) and Email servers. Unstructured data is everywhere and exploding. In modern organizations, unstructured data takes part in almost any mission critical business process. In most organizations it will contain sensitive information, trade secrets, internal financial data and other types of information that should be kept protected.

4.2 Securing Unstructured Data

[Rz 28] Unlike application oriented data, which is usually well mapped and has means of protection, unstructured data is loose and out of control. Organizations are now facing tremendous challenges:

- Map existing stores of unstructured data.
- Find data (folders, files, sites) owners and map key user groups.
- Classify sensitive data.
- Define and enforce authorization policies on data stores.

4.3 Structured & Unstructured Data Eco-Systems

[Rz 29] Unstructured data, in most cases, is only a subset of a more complete information collection. A quote document that is attached to a CRM record is more valuable and meaningful in that context. For that reason, some of these key challenges should be looked at from a complete, holistic approach. Keeping that concept in mind, organizations should not try to meet the unstructured data challenges with niche, isolated, tools that will evidently lead to a partial, incomplete solution.

4.4 Requirements for an effective solution

[Rz 30] The road to a complete solution that will provide actionable intelligence should contain the following milestones, at-least:

Category	Requirement

Access Monitoring	• Real time monitor of file/folder access with detailed audit trail • Real time monitor of permission changes with detailed audit trail • Source IP identification • Source User name identification • Support for Citrix/Terminal Services source identification • Support for any NAS platform • Leverage solution for other business assets monitoring (ERP, Mail, etc.) • Agent-less monitoring
Access Intelligence	• Complete visibility of effective folder/file permission with full visibility of groups, inheritance, etc. • Owner classification • Support for complete role (re-)engineering • Support for What-If scenarios • View Used/Unused permissions • Cross-reference with in place IT security policies and systems to better adapt access privileges to actual needs
Policy Compliance	• Granular Definition of security policies on files/folders • Leverage existing IT security infrastructure to define unified security rules • Automatically respond to violations
Workflow	• Support for an end-to-end user permissions review process • Support for regulatory attestation requirements

5 Conclusion

[Rz 31] Organizations today are using a variety of niche tools to fight the challenges of data governance. Organizations should tackle the Data Governance challenges within a DPMS with the «How can I track my user's activities and permissions?» question in mind. Organizations that only focus on the narrow «How can I track my file servers/NAS usage and permissions?» question will create a non-scalable solution that will have to be replaced, in the near future.

6 Literatur

Blumberg, Robert Atre, Shaku, The Problem with Unstructured Data, http://secs.ceas.uc.edu/~mazlack/ECE.716.Sp2010/DM.Review.Unstructured.Data/DM.Review.Discovery.1.pdf, last revised 12 January 2015

Bock, Kirsten, Rost, Martin, Privacy by Design and the New Protection Goals — Principles, Goals, and Requirements. Published in German in: DuD 2011/01, https://www.european-privacy-seal.eu/results/articles/DuD2011-01-RostBock-PbD-NSZ.pdf/view

Gerick, T. (2012). IT Analytics. Wege aus der Black Box. Retrieved March, 9th, 2013 from http://www.manageit.de/Online-Artikel/20120910/f.%20IT%20Analytics.htm

Johnson, Eric, Symantec Global Internet Security Threat Report, Trends for 2009, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf, last revised 12 January 2015

Maseberg, Sönke, Die datenschutz cert GmbH stellt vor: priventum — das Zertifikat für das Datenschutz-Management, in: certNews, article of 5 August 2010, https://www.datenschutz-cert.de/news/cert-news/beitrag/browse/9/bp/474/artikel/die-datenschutz-cert-gmbh-stellt-vor-priventum-das-zertifikat-fuer-das-datenschutz-management.html, last revised 12 January 2015

Rost, Martin, Grundlagen des Standard-Datenschutzmodells (SDM), mit Anwendung auf auf BigData, https://www.datenschutzzentrum.de/sommerakademie/2013/IB10-Rost_SDM.pdf, last revised 12 January 2015

Waters, John, Whitepaper, Unstructured Data Governance, Holistic approach to key challenges, 2012

Philipp E. Fischer, Ph.D. cand. (UOC Barcelona), LL.M. in Intellectual Property Law (Queen Mary University of London / TU Dresden); Data Protection Officer & -Auditor (TÜV), Managing Partner at SuiGenerisData GmbH, Münchner Straße 18, 85774 Unterföhring, DE,
pfischer@suigenerisdata.com, https://www.suigenerisdata.com
Ricardo Morte Ferrer, Ph.D. cand. (Zaragoza), Derechos Humanos y Libertades Fundamentales, Lawyer (Abogado), Master in Information and Knowledge Society (UOC), rmorte@arcor.de