GDPR entrapments. Proactive and reactive (re)design thinking

Willian Dimitrov

* University of Library Studies and Information Technologies (UNIBIT) Bulgaria,

Faculty "Information Sciences" (FIN), Sofia pk. 1784,

bul. "Tsarigradsko Shosse" № 119, e-mail: v.dimitrov@unibit.bg

Abstract. *It's clear that GDPR is leading to an explosion of business opportunities. Companies attempting to develop their own IT innovations are quickly learning that providing safe, secure, privacy-sensitive data interactions is extraordinarily difficult. The article explores opportunities of GDPR implementation, approaches, as far-reaching regulation that turn focus on security of ICT systems to data-centric view point, likely to be the central governing framework for consumer-oriented companies and generating new business models across the globe. The analisys of consequences proves the need for new design thinking paradigm concerning future ICT systems and massive reengineering of existing, if organization works with the personal information of anyone in the EU, whether based there or not, GDPR applies to it. The article can be useful to researchers, project leaders, ICT systems designers, developers, executives or decision makers involved with data management, risk, information security and data protection.*

The EU General Data Protection Regulation 2016/679 (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

The GDPR is intended to be one of the most contemporary regulations in a long time. That's lucky for all of us, since the internet of things is one of the fastest-moving technology and business spaces in a long time [16].

Introduction

The EU secondary legislation directives and regulations related to GDPR and in them have specific provisions on the application of the protection of personal data cover EU institutions, bodies, offices and agencies, the sectors of economy, health, services, education, finance, insurance, security, air and ground transport, e-government, communications, law enforcement, utilities - electricity, gas, heating, cybersecurity, trading companies, EURES network, servants, pension institutions and others.

This article aims predictions about issues and evaluate the challenges for organisations alined with GDPR at design, development and implementation.

Methodology and sources

For problem understanding are applied review, classification, analysis of Regulation 2016/679 and the documents resulting from it, systematisation of the challenges, comparison, empirical experience in the construction of information and communication technology security management systems.

Trusted digital relationships with users

To prepare for the GDPR, organizations need to go beyond data protection and embrace data transparency and data control. The choices about customers' data increasingly reflect on not just data protection officer's actions but on entire business model. Addressing user trust risks is certainly something you can do something about; the more important question might be whether you can afford not to [16].

What are the regulatory objectives of GDPR? Data privacy with choice and control: strengthening the exercise of fundamental privacy rights of individuals and putting users back in control of their personal data [16].

GDPR key changes

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although

the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies. The key points of the GDPR as well as information on the impacts it will have on business.

Increased Territorial Scope (extra-territorial applicability). Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. This topic has arisen in a number of high profile court cases. GPDR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Penalties. Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g.not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Consent. The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Data Subject Rights.

Breach Notification. Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access. Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten. Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Based on years of practical experience in deploying and supporting ICT security systems and researching data protection issues, I present a list and analysis of the potential traps spotted by control bodies and those who need to maintain compliance with the GDPR Regulation.

Data Portability. GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a '*commonly use and machine readable format*' and have the right to transmit that data to another controller.

Privacy by Design. Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At it's core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - *'The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'.* Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the

processing.

Data Protection Officers. Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications /registrations to each local DPA of data processing activities, nor will it be a requirement to notify/ obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices;
- May be a staff member or an external service provider;
- Contact details must be provided to the relevant DPA;
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge;
- Must report directly to the highest level of management;
- Must not carry out any other tasks that could results in a conflict of interest. [10], [17].

The article explore only technical aspects, without law regulation and organizational issues. Some of the technical issues, empiricaly established are given on *Table 1. List of GDPR entrapments.*

Detection Through Notification. The core of the incident response life cycle is detection, containment, analysis, and notification. One of the first issues many companies ask about is how fast notification should occur. Before a company is positioned to provide a meaningful notification, it needs time to stop the attack, determine who is affected, identify any appropriate measures to prevent a reoccurrence, and mitigate potential harm to affected individuals.

Very rarely is this possible within days or even a few weeks. To help identify realistic expectations on timing of notification, the report looked at four timing metrics. The overall average time to detect incident is 69 days and the median was 15 days. It is average amount of time from incident occurrence until discovery. The average time from detection until containment is 7 days. Analysis

Table 1

List of GDPR entrapments

DSR	Entrapments
Breach Notification	Many breakthroughs remain unknown forever; Are found by the clients of the companies; Are discovered years after they are realized .
Right to Access	Requires maturity of Identity Management solutions; Data subjects have to control their data in many repositories; User Controlled Access for Distributed data requires skilled end users; Dark data exists without governance and User Controlled Access
Right to be Forgotten	Distributed data are written in different data centers over the world; There exist data in old archives that are not encrypted; Dark data are hidden or it's not clear that it exist in cashes, forgotten file servers, data base engines and hosts in hipervisor environments, cloud services providers, social networks.
Data Portability	Central e-government data repository need to be in the game with GDPR; End user need to be trained to care after his data; End user need to have tools (interfaces) for operations caring his data.
Privacy by Design	Can't be applied to information, it's concerning data base design (SQL or NoSQL Shema), Data base engines and software applications architectures - One, Two, Three tiers, Distributed, SaaS, API and Libraries.
Data Protection Officers	Need to have expert knowledge on data protection law and practices and technical skill and knowledge about data on the move, processing data in progress and on the rest in the archives.

All companies are eager to complete the forensic investigation to determine the scope of an incident. On average, it took 43 days to complete forensic investigations. It is average amount of time from engagement of forensics until forensic investigation complete. Average amount of time from discovery until notification is 40 days.

There are, however, fraud resolution services, as

well as services that will monitor the "dark web" for signs that stolen data is being sold [11].

Dark data entrapments. The version of this part of the research I made in [28]. It suitet to the DPIA (data protection impact assessment) (Article 35) and can be implemented in the risk assessment where "The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing" (Article 39) [1].

Locations dark data resides. Depending on their expertise domain authors classified under term dark data different areas with structured or unstructured data.

- Emails, documents on file servers, social media, video and audio;
- Old files, data that is kept just in case, content on devices and clouds outside of IT control [25];
- Deliberately or accidentally hidden data in the file system – inside known hidden files, false bad clusters, intentionally hidden files [4];

There exist other dark data sources that are not mentioned in the studied articles and are the reason we introduce terms for explicit and hidden dark data. Those two types of dark data are defined based on the difference of their visibility from the owner's point of view.

Based on our experience in the field of different IT projects we can add to the existing list following sources:

- Hidden data in the files in a file system – old documents, pictures, scanned documents, filled pdf forms, notes on MS Word documents or handwritten notes on scanned documents, signed files and documents;
- Operating systems naturally generate data that can be easily classified as dark too: Non cleaned recycle bin in Windows, Linux and in UNIX. Memory cashes, disk cashes, and data base engines cashes, proxy's cache;
- Developing processes supporting data like sample test data sets, testing data base sets, real production data subsets dedicated for test provided to programmers and testers, which become dangerous after code freeze and everybody forgets about them;
- Application trails like web browser cache, bash history, encryption keys (e. g. supporting VPN or SSH), syslog records;
- Data located in forgotten virtual images installed or active in local hypervisors or cloud infrastructure;
- Data generated from different devices that are considered in the area of Internet of Things (IoT) – wearable or implanted devices communicating via Body Area Network (BAN) and gathered into mobile devices, sensors data from medical devices…
- Forgotten structured data that was created in different data base engines long time ago, nowadays nobody knows if they are in usage or not and no one takes care afterwards;
- Data that is in the desktop and mobile devices owned by contractors and customers, probably suited name is remote dark data.

Dark data can pose security risks in case it falls into the wrong hands, or becomes visible in the range outside its owner's control [26].

Dark data sources. The proliferation of dark data is partially the result of the "Bring Your Own Device" (BYOD) phenomenon, along with the continuing explosion of big data that includes new, unstructured data types such as audio, video, and social media. These practices create information governance challenges that arise when information is generated by and stored on mobile devices, social networks, file sharing services, and unmanaged SharePoint sites.

The unprecedented growth in data volumes and formats also plays a role, making it increasingly more difficult to discover, retrieve, and reuse trusted information. In this scenario, the business value of data is reduced, creating greater exposure and risk to the organization [8].

Some examples of data that is often left dark includes server log files that can expose clues to website visitor behavior, customer call details records that can indicate consumer sentiment and mobile geolocation data that can reveal traffic patterns to aid business planning [18].

Dark data hidden risks and potential data sea monsters. Specialists in IT, responsible for compliance with safety standards must be aware of the dark data located in the periphery of programs for managing change. This unmanaged, forgotten data can even hide outdated or inaccurate information that could be misinterpreted if discovered by auditors or lawyers.

All forms of electronically stored information (ESI) may become a subject to legal discovery if a threat of litigation emerges – even obsolete or incomplete data. The presence of uncategorized, unmanaged dark data can result in increased costs of the fid, review and analyze phases of discovery. Increased risks

may also result if dark data includes unidentified drafts or duplicates of documents that should have been disposed of in line with retention policies [19].

Legal Liability. A lack of insight into dark, unstructured or forgotten data could lead to financial or legal liability in addition to impacting your bottom line. Data covered by regulation that's kept but improperly stored can lead to costly sanctions for organizations. When this data is requested in court and cannot be located, the company may end up paying millions of dollars in fines. Regulatory risk are given in Table 2. Dark data risks.

Poorly categorized data may also lead to permissions challenges. Not knowing what each of your data sets contain creates confusion about who can access that data. If the wrong individuals are caught accessing sensitive information, it's putting the business at risk of a data breach [24].

Keeping all data in backup or archive systems may seem like a fail-safe, but if an organization doesn't know what data it is or where it is located, the cost outlays for storage and management will easily outweigh acceptable value. Enormous volumes of data lead to long backup windows and can make recovery operations time-consuming and extremely complicated

It's reasonable to the blurring of lines between PII (Personally Identifiable Information) and non-PII data. Case in point: it's been known for at least 10 years that there are specific pieces of data, which in isolation may appear anonymous, but when taken together they're just as effective at identifying a person as traditional PII.

The easiest way to understand these so called quasi-PIIs is the trio of full birth date, zip code, and gender. If a company published a dataset that had been "de-identified" by removing all the standard PIIs, but left those three data items alone, a smart hacker could find with a very high likelihood the name and address of the person behind that data [12].

To demonstrate just how easy, common and dangerous it is when data is improperly removed before used electronics are resold, the team [5] purchased a total of 200 used hard disk drives and solid state drives from eBay and Craigslist in the first quarter of 2016.

Here are the top findings from this study: 67% of the used hard disk drives and solid state drives hold personally identifiable information and 11% contain sensitive corporate data. Upon analyzing the 200 used drives, company emails were recovered on 9% of the drives, followed by spreadsheets containing sales projections and product inventories (5%) and CRM records (1%). 36 percent of the used HDDs/SSDs containing residual data had data improperly deleted from them by simply dragging files to the 'Recycle Bin' or using the basic delete button [5].

Table 2.

List of dark data risks

Risks	Explicit dark data	Hidden dark data
Intellectual property risks	will become clear after laborious research or intellectual property theft	It will not become clear until data are hidden or will become clear after intellectual property theft
Legal and regulatory risk.	Upon verification by authorities	If found during inspection
Business intelligence risks	If the data leak and fall into malicious actors	If the data leak and fall into malicious actors
Reputation risks	Will become clear after laborious research or security incident	It will not become clear until data are hidden or will become clear after security incident
Opportunity costs	Will become clear after laborious research	It will not become clear until data are hidden
Open-ended exposure	Poses unevaluated risks and damaged indeed	Developers and privileged users can enter data by accident
Confidentiality risks	PII, financial and sensitive data	leaked PII and sensitive data
Cyber security risks	If dark data contain information that reveal technical details for company IT	If bad guys found user names, passwords, tokens, crypto keys and so on

Privacy by design. Privacy by Design extends to a trilogy of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) networked

infrastructure.

Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of the privacy measures implemented tends to be commensurate with the sensitivity of the data.

The objectives of Privacy by Design are ensuring strong privacy and gaining personal control over one's information, and, for organizations, gaining a sustainable competitive advantage may be accomplished by practicing the 7 Foundational Principles, which are intended to serve as the foundation of one's privacy practices.

Proactive not reactive: preventative not remedial. The Privacy by Design (PbD) framework is characterized by the taking of proactive rather than reactive measures. It anticipates the risks and prevents privacy invasive events before they occur.

PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred it aims to identify the risks and prevent the harms from arising. In short, Privacy by Design comes before the fact, not after.

Privacy as the default setting. We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice, as the default. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual in order to protect their privacy — it is already built into the system, by default.

Privacy embedded into design. Data privacy regulations mandate specific guidelines on the classes of data to be protected including personal data, protected health information and financial data. IoT sensor data, geolocation codes, vehicle identification numbers (VINs) and IP addresses, along with many other data elements, qualify as sensitive personal data under the General Data Protection Regulation (GDPR) [13].

There's an explosion of new database technologies, and someone in the organization needs to stay abreast of what's available and what's the best solution to the problem at hand, someone with more diverse data literacy with different databases and languages. Given the growth and variety of options, it's rare for an enterprise to have the resources they need to analyze Big Data themselves. This has led to the growth of companies providing databases as a service (DBaaS), since these companies have the bandwidth to keep up with all of the latest technologies, know their strengths and weaknesses, and employ professionals who know the nuances of each database.

There were a number of skills mentioned by executives that make someone good at working with databases. These include: understanding the proper design structure, knowing what's in the database you're working with, and understanding data science and what data scientists are looking for. As the number of databases grow, it's important to understand the strengths and weaknesses of the different tools and to choose the right database for what you're trying to accomplish. More Big Data jobs are requiring a broader set of skills [20].

Lack of expertise among developers and overly complex libraries have led to widespread cryptographic implementation failures in business applications. The scale of the problem is significant. Cryptographic issues are the second most common type of flaws affecting applications across all industries, according to a report this week by application security firm Veracode. The report is based on static, dynamic and manual vulnerability analysis of over 200,000 commercial and self-developed applications used in corporate environments.

Cryptographic issues ranked higher in prevalence than historically common flaws like cross-site scripting, SQL injection and directory traversal. They included things like improper TLS (Transport Layer Security) certificate validation, cleartext storage of sensitive information, missing encryption for sensitive data, hard-coded cryptographic keys, inadequate encryption strength, insufficient entropy, non-random initialization vectors, improper verification of cryptographic signatures, and more.

The majority of the affected applications were Web-based, but mobile apps also accounted for a significant percentage [9].

In most system environments of the Cloud Service Providers (CSP), managing the security options for volume and storages will be a significant engagement because each client will need specific encryption options, data availability scenarios, and different types of access [14] [22].

The key encryption and management subsystem also has the important task of regulating the organization of processes. Experience with real installations makes us agree with James Randall that key management in the context of the ANSI X9 standard means generating, distributing, preserving over the life cycle, modifying requirements, setting ciphering startup values and message formats. The ANSI X9 specification, designed for financial institutions, contains a description of the life cycle management requirements

of the encryption keys [23].

Data in a network storage environment is significantly more vulnerable to unauthorized access, theft or abuse than data stored in the traditional, directly connected to the host storage. The college is not intended to divide the data contained in it, and the data from the different directorates and departments of the organizations remain mixed in the network [21].

Archiving data outside the organization can increase the risk of unauthorized access, both inside and outside the enterprise. For storage networks, a breakthrough in security could endanger the data of the entire organization [7].

One of the problems with Cloud computing is that both the CSP and law enforcement can access files, usually easier than if customers store them on their own computers [3].

The security of a cryptographic system depends on the control of the cryptographic keys and the components of these keys. Responsibility for key management is currently the Cloud computing customer organization. The generation of storage keys is usually performed outside Cloud through hardware modules, which does not fit completely into the Cloud paradigm.

The basic principle is that the organization controls the encryption keys and configures the key management modules. Prior to using the key management department's CSP services, the organization needs to understand in depth and weigh the risks associated with the life-cycle management of key encryption provided by the CSP [15] Cryptographic operations performed in CSP infrastructures are part of the overall process of key management and should therefore be controlled and audited by the client organization [27].

Despite the KMIP and IEEE P1619.3 interoperability standards for key management in cryptographic systems by different manufacturers in [2], many opinions have been summed up to confirm the notion that in the coming years there will be no rigorous solutions for the management of cryptographic keys that are suitable for application in Cloud and maintain the required level of interoperability [6].

Results and recommendations

The conclusions based on listed entrapments. As Consequences the corporate policies, development methodologies, system design approaches, integration projects, e-government structures, telecommunications, utilities and businesses operation with EU sitizens data need to transform organizational processes, security and data protection technologies and professional staff education and training can be aligned with GDPR requirements. In general the companies over the world operating with EU sitizens data need to be in compliance with GDPR despite local regulation for example Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM) and others.

Development methodologies from waterfall to contemporary Kanban, DevOps, Agile Scrum need to be upgraded according GDPR requirements. The same requirements are for pgraming languages, programing libraries, API, and software testing.

Standards like CMDB, ITIL, ISO 20000 can be implementetd taking into account GDPR articles.

Organisations in compliance with ISO 27000, COBIT, SOX need to do audits, data minimization and take additional actions toward GDPR compliance.

Guidelines for future research

Possibilities for future research are GDPR innovation-friendly rules. They are a guarantee that data protection safeguards are built into products and services from the earliest stage of development, the approach for data protection by design and by default [10], [17].

In my opinion Human Resources Entrapments are more dangerous than others because of sophisticated social ingeneering approaches today combined with phishing and information about companies spread through internet content infrastructure in general and social networks.

ACKNOWLEDGEMENTS

This work has been developed following the activities of project "Conceptual and Simulation Modeling of Ecosystems for the Internet of Things (CoMein)", funded by the Bulgarian Scientific Research Fund, Competition "Fundamental Research - 2016", (Contract ДН02/1/13.12.2016г.)

SOURCES

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

[2] Encryption key management is vital to securing enterprise data storage. *Computer Weekly*, February 2010.

[3] http://www.cloudswitch.com/page/is-encryption-the-solution-to-cloud-computing-security-and-privacy. *Is*

Encryption the Solution to Cloud Computing Security and Privacy?, August 2011.

[4] Hal Berghel, David Hoelzer, and Michael Sthultz. *Chapter 1 Data Hiding Tactics for Windows and Unix File Systems*, volume 74 of *Advances in Computers*. Elsevier, 2008.

[5] blancco. The leftovers: A data recovery study, June 2016.

[6] Oracle Chairs:Tony Cox (tony.cox@cryptsoft.com) Cryptsoft Saikat Saha (saikat.saha@oracle.com). Key management interoperability protocol usage guide version 1.3.

[7] Decru A NetApp Company. Evaluating a storage security solution. considerations and best practices for securing sensitive data. November 2006.

[8] L. P. Hewlett-Packard Development Company. Gain control over legacy data. hp legacy data clean-up solution., 2013.

[9] Lucian Constantin. Software developers aren't implementing encryption correctly, 2015.

[10] eu.gdpr.org. Gdpr key changes. an overview of the main changes under gpdr and how they differ from the previous directive, http://www.eugdpr.org/key-changes.html.

[11] BakerHostetler Theodore J. Kobus William R. Daugherty Gerald J. Ferguson. 2016 data security incident response report.

[12] Andy Green. Revealed: Secret piis in your unstructured data. http://blog.varonis.com/revealed-secret-piis-in-your-unstructured-data/, mar 2013.

[13] Reiner Kappenberger. Protect iot data with fpe to monetize it. *http://itknowledgeexchange.techtarget.com/iot-agenda/protect-iot-data-fpe-monetize/*.

[14] Matt Sexton Karen Scarfone, Murugiah Souppaya. *Guide to Storage Encryption Technologies for End User Devices*. Recommendations of the National Institute of Standards and Technology, November 2007.

[15] Paul Hoffman Karen Scarfone, Murugiah Souppaya. *Guide to Security for Full Virtualization Technologies*. Recommendations of the National Institute of Standards and Technology, January 2011.

[16] Eve Maler. Gdpr: ItвЂ™s more than a regulation, itвЂ™s an opportunity. *http://itknowledgeexchange.techtarget.com/iot-agenda/gdpr-regulation-opportunity/*.

[17] Adopted on 13 December 2016. Article 29 data protection working party 16/en wp 243. *Guidelines on Data Protection Officers*.

[18] Margaret Rouse. Dark data. In *http://whatis.com*. http://whatis.com.

[19] L. L. C. Viewpoint Archive Services. Dark data, big data, your data: Creating an action plan for information governance, apr 2013.

[20] TOM SMITH. Executive insights on data persistence, 2016.

[21] Storage Networking Industry Association (SNIA). Starage security industry forum. *SSIF Solutions Guide for Data-At-Rest*, 09-0401, 2009.

[22] Sophos. http://www.sophos.com/en-us/support/knowledgebase/107852.aspx. *Distinguishing between opal-, volume- and file-based encryption on the SafeGuard Enterprise Client*, Article ID: 107852, 2011.

[23] ANSI X9 Financial Industry Standards. Cryptographic key management. http://xml.coverpages.org/keyManagement.html, August 2013.

[24] Richard Stiennon. Are dark & unstructured data putting your business at risk?, https://www.blancco.com/blog-dark-unstructured-data-business-risk/?platform=hootsuite.

[25] Hitachi Data Systems. Big data - shining the light on enterprise dark data (edd), apr 2013.

[26] Ed Tittel. The dangers of dark data and how to minimize your exposure. *CIO*, http://www.cio.com/article/2686755/data-analytics/the-dangers-of-dark-data-and-how-to-minimize-your-exposure.html, sep 2014.

[27] Timothy Grance Wayne Jansen. Guidelines on security and privacy in public cloud computing. *NIST Special Publication 800-144*, December 2011.

[28] University of Library Studies Willian Dimitrov and Sofia: Dark data governance reduces security risks, Information Technologies. *BdKCSE'2016" Big Data, Knowledge and Control Systems Engineering*, 2016, December.