Implications of EU-GDPR in Low-Grade Social, Activist and NGO Settings

Lars Magnusson[1], Sarfraz Iqbal[1]

[1]Universitetslektor, Department of Informatics ,Linnaeus University
351 95 Växjö, Sweden
lars.mson@gmail.com, sarfraz.iqbal@lnu.se

Abstract. Social support services are becoming popular among the citizens of every country and every age. Though, social support services easily accessible on mobile phones are used in different contexts, ranging from extending your presence and connectivity to friends, family and colleagues to using social media services for being a social activist seeking to help individuals confined in miserable situations such as homeless community, drug addicts or even revolutionists fighting against dictatorships etc. However, a very recent development in the European Parliament's law (2016/679) on the processing and free movement of personal data in terms of EU-GDPR (General data protection rules) considers the low funded social service development efforts unsafe. This article analyses a case study conducted at a shelter for homeless mothers in the United States to conceptualize the future similar development efforts from low end public activist groups within European union. This article aims to raise awareness on this issue and also puts forth a conceptual model to envision the possibilities of mitigating the risks attached to such development efforts under the light of EU-GDPR which will be implemented in may 2018.

Keywords: GDPR, social services, information security, public activist

Introduction

Information security refers to the protection of data, information and information systems from unauthorized access, disclosure, disruption, modification, or destruction in order to maintain integrity, confidentiality and availability [1-3]. A recent data breach investigation report [4] discloses that over 100,000 security incidents were reported from 82 countries, including 3141 confirmed data breaches. To improve protection, in April 27, 2016 the European Union passed the new European data protection regulation, General Data Protection Regulation (GDPR) [5], as the successor to the 1995 Privacy Data Directive [6]. One of the main reasons to propose the new regulation was that most member states never implemented the 1995 directive completely. The earlier lawmakers did not anticipate today's more forceful data processing landscape, making the old directive less useful as a tool to regulate the security of the EU citizens' personal data [6].
The new regulation, GDPR, attempts to adopt a stance more in line with today's data processing requirements, both restricting as well as simplifying for a Data Collector to intuitively arrange and collect data needed in accordance with the new regulation [5]. Clear rules to adapt to, easier to do, EU "in-house" offshoring and to understand the data owners' rights. GDPR has moved the right of data ownership from the Data Collectors to the Data Object. This is a ***key*** element of the new regulation, where an EU resident have been asserted a number of rights, regarding any data describing the intended individual (data object) such as:

A. The described individual is the sole owner of any data describing him or her
B. It does not matter where in the world such data collection is performed
C. Apart from defined areas like military, law enforcement and/or healthcare information (where national exemptions may exist), the data owner has the right to request his/her data to be reviewed, destroyed or moved entirely to any competing IT services. Destruction is under the rule of "The right to be forgotten".
D. Data regarding residents under 16 years of age is seen as extra sensitive
E. Data regarding legal or healthcare information, sexual orientation and "race" is equally sensitive.
F. Data Collector need to have a direct free and clear consent, in some cases a non-repudiable consent from the data owner to process his/her data.
G. Data Processor helping Data Collector is equally responsible to follow GDPR
H. Data Collector and Processor need to have data securing controls in place, not to lose the data stored and/or processed.
I. Lost data has to be reported within 72 hours to the national overseer in the member state where the loss occurred or country overseeing the processing. Provision to notify the data owners also exist
J. If data loss takes place, and responsible people fail to notify the overseer within the allotted time, both these conditions can induce EU fines up to €20M.

Apart from the above listed conditions, there are other important conditions such as, how to secure data according to "Security by Design and Default" [5] with "who did what, when, where and why" controls. All this means, the board of directors or top management need to review GDPR regarding the daily operations of organization. GDPR is a board level issue, not an IT department issue. The authors of this article has concentrated on how it will pan out, reviewing the increased use of cheap mobile applications and communication within support services of a social context, activist groups and NGO organizations. This article attempts to see a more practical approach on how such social support services / initiatives can be implemented for the target audience under the umbrella of GDPR. How such initiatives could be implemented without breaking GDPR. This article intends to develop that thought, looking at a possible framework satisfying GDPR requirements for low-grade social, activist and NGO-like organizations or groups.

The remainder of the article is arranged as follows. Section 2 provides a brief case description. Section 3 provides an overview of case analysis and GDPR effects on the organizations involved in low-grade social support services development. Section 4 highlights critical GDPR control objectives. Section 5 introduces a conceptualized best practice framework for personal data. Finally, section 6 provides a brief discussion and suggests further research.

Case Description

Social support groups acquire a lot of contact information and in cases of innovative social services development; these can be labelled as extra sensitive. Such low-grade service development is currently more seen in U.S. than in Europe, so our guiding case which we analyzed in this article has been one by Georgia Tech from 2008 [7] with a follow up in 2011 [8]. In this case, a team under Cristopher le Dantec aided a local "NGO" in Georgia to set up a SMS based support service to help a number of poor and sometimes addicted-substance and/or abused mothers at a shelter. When out of the shelter, the mothers used the SMS service to keep in touch and follow up meetings with personnel at the shelter as well as supporting healthcare instances.

It was reasonably secure to use mobile services in U.S. at the time, when this study was conducted. Likewise, these types of low-grade social support efforts are important, since they do support a governmental expectation to help socially weak persons in the society, giving them a more "anonymous", indirect interface to a support they otherwise might avoid [7]. A support many EU nations would like to see here. Nevertheless, with a lot of conflicting issues with regards to GDPR [5], how can we build such services in Europe, without colliding with the pending regulation?

Case Analysis and GDPR effects on the organization

In the assumed case of a similar local initiative in an EU country, outside or partly outside the control of any guiding public framework, the leadership has to create their own controls to satisfy GDPR's requirements. An absolute necessity, since GDPR covers organizations of all sizes, ranging from 2-3 person operations to thousands of employees [5]. In some cases, not only so called "mom&pop" operations [9], but also one/two-person operations, if the data processed is requiring this protection.

Our assumed case is however a social support services group with the size of maybe 15-20 persons, one locality, hires it's IT services and operates with a low budget. Most of its budget goes to support the clients. Duplicating the Georgia case [7, 8] as a single mother shelter in a larger European city. The analysis under the light of GDPR shows that there are a number of conditions to consider:

Leadership understanding and responsibility – GDPR compliance in an organization is typically a work performed under supervision of the organizational Legal Officer and the now mandatory Data Protection Officer (DPO), a structural work effort, to adhere to the regulation (in case, if employees are more than 250 or data processed is regarded sensitive). Not having a described compliance process with responsibilities could lead to penalties, when audited.

Leadership strategy – GDPR [5] requires the leadership of our shelter to review its operations from a new perspective. It can potentially be subject to fines amounting to €20M (amounts this type of organization isn't close to possess). Leadership therefor has to establish a strategy of minimizing risks, both within the organization and supporting IT services. It has to negotiate responsibility with the IT services, the shelter being the Data Collector and the IT services being Data Processor, with contractual terms aligning to the regulation. They need to specify rules and strategies regarding handling of the personal data, such as "The right to be forgotten" [5]. Not at technical level, but at a strategic level. Some European member states do have healthcare laws, nullifying for instance "The right to be forgotten" regulation [10]. If our organization provides some services within that legal framework, they have to abide to that law instead of GDPR.

Internal Control - The leadership also need to establish an internal framework that supports work with internal control. Thus, everyone follows the rules and pose no risk to the client's data. It is not completely new, but now there is support for more active auditing, independent of internal or external contract, including documentation of actions and decisions to implementation of personal data collection or treatment of personal data. GDPR unavoidably increases the administrative work; however, implementing a working change control, this can double as a decision and operational record. ITIL [11] is currently not intended as such, but as basis tracking of decisions for GDPR, ITIL presents a workable solution.

Need of a DPO – Our case organization is far too small to have a resident DPO [5]. At the same time, it collects high risk data from several perspectives. Estrange spouses wanting to find a sheltered wife, others seeking information or in other ways coercing a client to something. Therefore, a part-time DPO, coming in a couple of times per year could be recommended.

Financing GDPR corrective actions – This is the leadership's most challenging issue, GDPR is about data security and maintenance, two topic areas typically of lowest importance on the Chief Finance Officer's (CFO) list. These issues need to be raised to the board level considering GDPR's penalty structure.
Organization's familiarity to GDPR – As with any information security work, we need to align the organization with the regulations and controls we are to operate within. It is a well-established fact that the need of policy and practice framework (P&P) is essential for acceptance of information security practices [12, 13, 14] and that it has to be validated by the leadership. If not, the P&Ps' will fail [15]. We need to invest in training people for GDPR and information security [16].
Data consent, collecting privacy data – GDPR is very consistent regarding to inform the data owner what data we intend to collect and the way we intend to process it. It is a clause of transparency. It also debates the form for getting the consent from the data owner. We need exemplary court cases to clear some ambiguous wording in the regulation regarding the need for non-repudiate able approvals.

Critical GDPR Control Objectives

Control objectives aim to support and highlight topics and actions to follow up the different aspects of GDPR affecting our small case organization such as:
Avoid unnecessary collection – Due to GDPR's data mapping requirement [5], "good to have" data cannot be collected any more. Organization need to actively analyze what it wants to achieve and what data is needed for that purpose. All other data should be de-selected and avoided to collect. Data used need to be documented, why and how as well as from where it is collected. A complete audit trail to prove that the organization do not collect nor process data outside the consent of the data owner [5].
Who accessed what and when – GDPR can be condensed to the sentence "Who did what, when, why and where" [5]. GDPR expects that due to the demand "Security by Design and Default", we have total control and tracking of the data to process and store. Thus, only those with 'work need' can access the data, all others denied. Rules for access need to be documented for future auditors to see how the thoughts behind a certain access were derived.
Reducing breaches via mobile app or web sites – The whole idea behind le Dantec and his team's design was mobility and easy access. However, a large part of our mobile applications leak substantial amounts of data, both intentionally and unintentionally. Researchers such as Mansfield-Devine [17, 18] and Snyder [19] point out a lot of deficiencies in the mobile sector, mostly due to a lack of motivation for developing the applications accurately as per recommendations of Open Web Security
Project (OWASP.org) and SANS Institute (Sans.org). Memory handling and on-unit storage should be encrypted, not to leak data to other apps scanning the phone/tablet. [17, 18, 19].
Secure communications and critical applications – All applications, also central ones, handling personal data, should always communicate over encrypted lines, either application to application or server to server communications. To use network protocols like ftp or http is directly against GDPR [5]. This is not new, both the international banking standard PCI-DSS [20] and the US finance regulation Sarbanes- Oxley Act of 2002 [21] has already regulated against use of unsecure protocols. The leadership has the responsibility to secure that these deficiencies and breaches to "Security by Design and Default" demand do not exist. The basic rule is the universal network rule "Deny all, allow needed". Not following it, is a professional failing.
Necessary logging – One specific aspect in the light of the US Target Group [22], Equifax [23] and Deloitte [24] hacks, is that we do track people and traffic. It is a delicate balance between

the individual's rights and security needs, but as the Target hack showed, we need to see changes in the traffic and infrastructure to stop attacks. Which requires logging, with logs for at least 6 to 9 months. A security report from 2016 [25] declares that average time to disclosure of a hack was 205 days. It was down from over 430 days in 2011, but still, with too short logs, we will miss anomalous events.

Emergency and continuation procedures – A task often labelled as un-necessary cost. IT is by leadership mostly regarded as a service function. At the same time, how long does an organization survive and can work, without IT? IT has become the "blood stream" of all organizations, so any lack of a DRP plan is critical. Maybe not a core issue for GDPR, but during a disaster, servers could be put out on the street to clear facilities. If their disks contain personal data, this could be a criminal spread of such data. Figure 1. Key Aspects handling GDPR

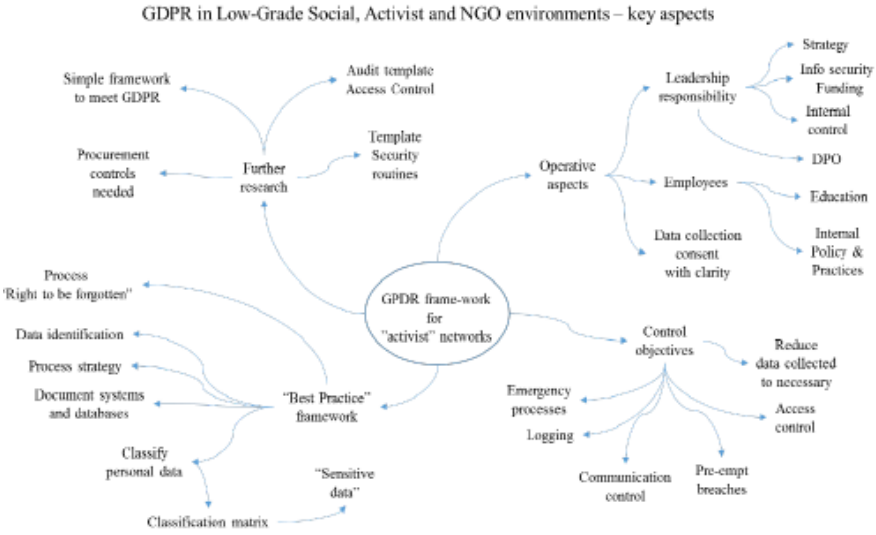

Figure 1. Key Aspects handling GDPR

Conceptualized Best Practice Framework for Personal Data

A key component in handling GDPR, is to know what personal data we have and where it is located. Answering the auditor "we have no idea", can be very expensive. We have to perform an inventory, including a data map, a map that need to be a live document, as our data flows and storage changes.

Identify and inventory existing personal data

A. List all systems and databases containing personal data, tagging sensitive data
B. Identify all internal and external data sources and associated communication
C. Implement a classification matrix and classify existing data and files accordingly
D. Review if consent for storing and using the identified data exist per data type
E. Create strategy for handling sensitive data, such as underage object, info about health, sex, sexual orientation, "race", political orientation, group memberships
F. Create strategy to handle "Right to be forgotten" and data transfer or "past best date" deletions. Conditions that can induce top penalties if not followed.

Although, all these are non-IT actions, they act as basic fundamental rules to identify if the organization have a right to collect and store the existing and planned information as per GDPR's requirements [5]. When all the data is reviewed and evaluated (including creating a classification matrix), the leadership together with the Legal Officer or any legal representation available as well as with the part-time DPO, need to discuss the future of the material and processes to keep in line with GDPR. GDPR demands a thorough audit trail, to see why a decision was made and by whom. Thus, the decisions to proceed need to be properly documented.

Discussion and Further Research

GDPR focuses mainly on the security and maintenance of data. It is evident that the EU politicians want to create incentives for creating state-funded and/or NGO driven support functions, similar to the case described above (see section 2-4). They see a need even in Europe and therefore have some provisions in both GDPR [5] and in the NIS directive [26]. GDPR motivates those developing applications, to know the security recommendations and programs appropriately, otherwise they do risk a 2% penalty of their global turnover. In this article, we endeavored to review the effects of GDPR with regards to development of low-grade social support services. The research work is on-going and we see further need to exemplify how these social support groups can follow the GDPR by outlining an initial GDPR Best Practice Framework both for processes and technology. The topics include, but are not limited to: Access control process, Security processes, Rules for in-house development of IT support and Procurement framework to support GDPR enabled solutions. We hope that the research community can help these cash-strapped groups with information, leading to best practices to increase their security awareness and measures so that such endeavors does not foil due to incidents as related by Verizon [4] and Madiant [25].

References

1. J. McCumber, "Information systems security: A comprehensive model," in Proceedings of the 14th National Computer Security Conference, 1991.
2. J. K. Tudor, "Information Security Architecture: An Integrated Approach to Security in the Organization," CRC Press Inc Boca Raton FL USA, 2000.
3. "Standards for Security Categorization of Federal Information and Information Systems." Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900, 2004.
4. Report "Verizon 2016 Data Breach Investigations Report", Verizon LLC, NY,US, as viewed Sept 10, 2017:http://www.verizonenterprise.com/resources/reports/rp_ DBIR_2016_ Report_en_xg.pdf
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Bruxelles, May 10, 2016.
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Bruxelles, Oct 24, 1995.
7. Le Dantec, C.A., Farrell, R.G., Christensen, J.E., Baily, M., Ellis, J.B., Kellog, W.A.,Edwards, W.K., 2011, "Publics in Practics: Ubiquitous Computing at a Shelter forHomeless Mothers", ACM/CHI, May 7-12 2011, Vancouver, BC, Canada