Enabling Privacy by Design in GDPR: An Analysis of Industry Tool Support

Smirity Kaushik
SALT Lab
School of Information Studies
Syracuse University
Syracuse, NY 13244, USA
smkaushi@syr.edu

Yang Wang
SALT Lab
School of Information Studies
Syracuse University
Syracuse, NY 13244, USA
ywang@syr.edu

Abstract

The European Union- General Data Protection Regulation (GDPR) will bring about a sea change in the protection of user privacy. On 25 May 2018, the 28 member states of EU will adopt GDPR as a legal mandate. However, the impact of GDPR will resonate throughout the world as it will affect every organization (both public and private) globally that captures or processes the personal data of EU citizens. GDPR is a vast regulation that covers provisions related to concepts such as user consent, right to be forgotten, and privacy by design and by default. It is for the first time that privacy by design, a well-recognized industry best practice, has been included as a legal requirement in a regulation. This paper gauges the industry readiness to adopt PbD in the context of GDPR by analyzing the tools offered by privacy vendors from a HCI standpoint.

Author Keywords

GDPR, Privacy by design, Tool analysis, Privacy

Introduction

The innovation cycle of the modern information society [8] is rapidly evolving. Law needs to catch up with the technology to safeguard the user privacy on the internet. European Union, General Data Protection Regulation (GDPR) [1] is a strong step towards regulating the processing of personal data of the EU citizens. On May 25 2018, GDPR will directly

25(1): Data privacy by design means that appropriate organizational and technical measures to ensure personal data security and privacy are embedded into the complete life cycle of an organization's products, services, applications, and business and technical procedures. Technical measures can include, but are not limited to, pseudonymization and data minimization.

25(2): Data privacy by default means that (a) only necessary personal data is collected, stored, or processed and (b) personal data is not accessible to an indefinite number of people.

Article 25, GDPR

apply to all 28 member states of the European Union, replacing the 1995 Data Protection Rules (Directive 95/46/EC). The key goal of GDPR is to give users control of their data and to create trust in the society so that the digital economy can grow [14]. The GDPR introduced the Privacy by design concept for the first time as a legal requirement [6] under Article 25, Privacy by design and by default [2]. Article 25 directs the controllers/processors to implement PbD concept and fulfills the key requirements of Article 5 (Principles relating to processing of personal data) [4].

At it's core, Privacy by Design (PbD) calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition [6]. It was introduced by Ann Covoukian in the mid 90's to address the growing issues of the information and communication technology [9]. She also introduced seven Privacy by Design principles and have since then become IT industry best practices.These are as follows [11]:

- Proactive not Reactive; Preventative not Remedial
- Privacy as the Default
- Privacy embedded into the design
- Full functionality - Positive-sum,not Zero-sum
- End-to-End Security – Full Lifecycle Protection
- Visibility and Transparency – Keep it Open
- Respect for User Privacy – Keep it User-Centric

At the policy forefront, the concept of PbD loosely associates with the 8 core principles for processing of data [6], namely, 1) Collection limitatiion 2) Data quality 3) Purpose specification 4) Use limitation 5) Security safeguard 6) Openness 7) Individual participation 8) Accountability These principles were first proposed by Organisation for Economic Co-operation and Development (OECD) in its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1983) [7]. Later these were adopted in the EU's 1995 Directive. However, since both the OECD guidelines and the Directive were non-binding in nature, the principles could not be effectively implemented in all the member states. Hopefully, with the onset of the strong and binding regulation such as GDPR, PbD as a legal requirement will be effectively implemented in the member states and create global impact through industry wide use.

In this paper, we have attempted to gauge the industry readiness to effectively implement PbD concept per the GDPR Article 5 and 25. The process analyzes the user privacy protection tools offered by 28 leading privacy vendors in the market. These privacy vendors are often used as customer off the shelf (COTS) third-party vendor tools by the companies (Controller (Article 4(7) or Processor (Article 4(8)) that capture, stores or process personal (Article 4(1)) or sensitive data (Article 9) [5] of the end-customer (Data user: Article 4) [3]. The analyzed tools are further classified into three categories on the basis of features offered, requirements of Article 25, 5, and the scope of interaction with the end-users, giving them flexibility of sharing data and data ownership.

Method

The research process is divided into three parts. In the first part, we conducted a deep analysis of the GDPR and created a regulation framework. The second part included the analysis of the privacy vendors available in the market and to map their tool offerings to specific article of the GDPR in order to create a big picture. In the third phase, we

Principles relating to processing of Personal data:
5(1)(a)- Lawfulness, fairness and transparency of processed data
5(1)(b)- Purpose limitation of personal data
5(1)(c)- Data minimization
5(1)(d)- Data accuracy
5(1)(e)- Storage limitation
5(1)(f)- Integrity and confidentiality of processed data
5(2) - Accountability.

Article 5, GDPR

filtered tools that specifically addressed the Privacy by design requirements per Article 25 and 5 of the GDPR.

Regulation analysis
We analyzed the General Data Protection Regulation in detail using the primary source document, i.e. the Regulation itself and divided it into 8 categories. Each category contain a group of articles related to a central theme. These categories are as follows:

- Governance (Fair and Lawful processing - Article 5, 6, 9, 27, 89, 37, 38, 39)
- Consent Management - (Article 4(11), 6(1)(a), 7, 8, 9(2)(a), 13(2), 14(2), 49(1)(a))
- Data Subjects rights - (Article 12, 15, 16, 17, 18, 19, 20, 21, 22)
- Data Breach Notification - (Article 32, 33, 34)
- Accountability - (Article 5, 24, 25, 26, 28, 29 30, 35, 36)
- Notices /Vetting - (Article 10, 12, 13, 14)
- Independent Supervisory Authorities - (Article 51- 56)
- International Data Transfer - (Article 44- 50)

We also analyzed the GDPR frameworks provided by secondary sources. Once the analysis of the regulation was completed, the second step was to map the third party privacy vendor tools to each of the articles of GDPR in each of the 8 categories.

Vendor Assessment
The sources list for the vendor assessment was picked from the IAPP 2017 Privacy vendor report [12]. A total of 55 vendors were assessed and mapped against the GDPR articles. The process of assessment involved analyzing the white-papers and other resource materials offered on the websites of the vendors. For the purpose of this paper, 28 vendors were filtered from four major categories: Accountability (Article 25, 24), Consent Management (Article 6, 7), Data subjects rights (Article 12, 16, 18, 19), and Governance - Fair and Transparent data use (Article 5, 9). A deep analysis of the website and the white-papers of the these 28 vendors was conducted to understand how they implemented Privacy by design (PbD) concept.

Findings:

Our analyses suggested that 28 privacy vendors integrated Privacy by Design (PbD) concept into their tools offering. Since PbD is a vast concept, we classified the features offered by the vendors into three broad categories on the basis of features offered, requirements of Article 25, 5, and the scope of interaction with the end-users. These categories are:

- Tools offering encryption, anonymization, pesudonymization and other embedded security features to safeguard user's Personal Identified information (PII) and Personal health information (PHI) [5]
- Tools offering an overview to the user of all the third-party websites tracking them and giving them an option to opt-in or out of the cookies and third party trackers.
- Tools offering opt-in and opt-out features to the end-users to share their data with the controller

through an interactive mobile application or web platform.

Next, we will discuss each category in more details.

Processing of personal data (racial, political opinions, religious, or trade union membership), genetic data, biometric data, health related data or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Article 9, GDPR

'Pseudonymisation' means the processing of personal data in such a manner that it can no longer be attributed to a specific data subject without the use of additional information

Article 4(5), GDPR

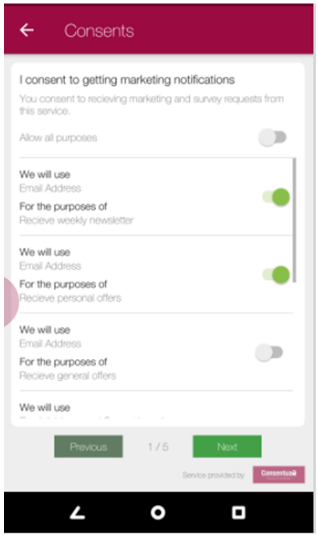
Category 1: Encryption, anonymization, pesudonymization and other security features
The tools in this category, by design and by default, protects data using enhanced visibility into any sensitive data flow and access controls across the controller platform. Once the risk analysis is performed, the vendor tools implement controls to secure sensitive user data using encryption, blocking, quarantining, anonymization and pseudonymization including blanking, hashing, replacement lookups, number randomization and masking. By transforming the sensitive user data into depersonalized data, these vendors successfully achieve compliance with the Article 25, 24, 9 and 5. Within this category, there are mild variations in features offered by various vendors. For example, Wizuda [13] not only provides anonymization and pesudonymization (definition Article 4, GDPR [3]) of user sensitive data but also provides user-friendly online previews to enable users to see the changes applied to their sample data so they can ensure they are happy with those changes, prior to confirming. In another example, Virtru [10] provide email encryption features to both the organizations and the end-customers respectively. The version available for the end-customers includes features such as option to encrypt emails, disable forward, set expiration, and revoke sent messages.

Category 2: Notice and control features for third-party data practices
The tools in this category offer features that gives the end-users an overall view of the cookie and third party trackers that may be potentially tracking the sensitive information of the end-user for the purpose of marketing and targeted ads. The tool is embedded in the user-interaction platforms such as website/ mobile application of the controller. The tools provided by these vendors help the controllers/processors become compliant to not only Article 25 but also Article 6 and 7 (User Consent) of GDPR.

A good example of this type of feature is offered by OneTrust [18]. It embeds consent management directly into organization's website, devices, and internal systems and scans the cookies and the third parties that are tracking the user information. It then creates a cookie banner for users and provides them with the option to opt-in or out of the cookie trackers. It also provides forms to the users to exercise Article 15 to 21 [1], receive notification when a request has been submitted, and automatically request an extension on the organization's behalf, if a deadline approaches. From the organization's standpoint it provides a list of information that users have consented to share with the cookies and third party trackers. In another example, Baycloud [16] offers five privacy consent management tools that directly interact with end-customers These tools help the users to see which third party websites are tracking them online and allows the users to change the consent to these third parties to track them.

Category 3: Notice and control features for first-party data practices
The tools in this category offer the consent management services to the controllers and works at the cross section of user interaction with the organization tools. They integrate across the existing platform of the organization such as Customer relationship management tools, Campaign Management Tools, and other system that directly interact with the end-users and capture their sensitive data.

As an example, Consentric [17] is a personal data



Consents

I consent to getting marketing notifications

You consent to recieving marketing and survey requests from this service.

Allow all purposes

We will use
Email Address
For the purposes of
Recieve weekly newsletter

We will use
Email Address
For the purposes of
Recieve personal offers

We will use
Email Address
For the purposes of
Recieve general offers

We will use

Consentua user consent interface [15]

Communications with data subjects must be transparent, clear and easily understood.
Article 12, GDPR

management platform that offers three key solutions for the organizations - Engage, Value Index and Permission. Engage captures data in real time and Value Index helps in managing the big data of the organization. Permissions provides transparency to the customers by letting them manage their own data usage and sharing permissions. Moreover it provides digital management for data consent and manages online permissions for the controllers, using real-time data capture and machine learning.

Another consent management vendor, Consentua [15] provides extensive control to the users over the information they wish to share with the concerned organization. It provides users with a choice to opt - in or out of the services of the organization either completely or partially. It also lays down the purpose for which a particular PII of the user will be used within that service. For example, in providing customized marketing services to the user, the interface displays the PII that will be collected, in this case the email, and the purpose for which it will be collected, in this case for receiving weekly newsletters. Organizations deploy Consentua within their own applications via some easy to use APIs to capture the consent of their users. Consentua allows organization to become compliant with Art 5, 25, 12 and 7 of GDPR [1] by providing users a choice to share only the most relevant information. It also highlights the purpose for which that information is being collected in an easy to read format (a requirment under Aticle 12).

Discussion and Future Work

Our findings reveal that the market for implementation of Privacy by design concept is in the development stage. 26 out of 28 of the privacy vendors provide tools that focus on encryption of the user personal and sensitive data. These tools do not involve direct interaction with the end-user. Only minority of tools (10 out of 28 vendors) provide transparency features to the users per the Article 5 and 25. These tools directly interact with the end-user and provide them flexibility of sharing their personal and sensitive data based on their choice through the opt-in and opt-out functions. They also show users which third party websites are tracking their data for the purpose of direct marketing and targeted ads. However, the limitation of our findings is that the analysis of these tools was based purely on the review of their white-papers. The demo of these tools has not been conducted to test the effectiveness of their capabilities.

Our results shed light on future research opportunities on this topic. HCI community can contribute in the area of evaluating the usability of user-interactive features of the tools offered by the privacy vendors. Habituation and scalability could also present as challenges for these features, similar to other privacy and security user interface.

REFERENCES

1. 04-05-2016. 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). *OJ* L 119/1 (04-05-2016), 1–88.

2. 2017a. Article 25 EU General Data Protection Regulation EUGDPR PrivacyPrivazy according to plan. `http://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm`. (2017). (Accessed on 2/2/2018).

3. 2017b. Article 4 EU General Data Protection Regulation EUGDPR PrivacyPrivazy according to plan.

http://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm. (2017). (Accessed on 2/2/2018).

4. 2017c. Article 5 EU General Data Protection Regulation EUGDPR PrivacyPrivazy according to plan. http://www.privacy-regulation.eu/en/article-5-principles-relating-to-processing-of-personal-data-GDPR.htm. (2017). (Accessed on 2/2/2018).
5. 2017d. Article 9 EU General Data Protection Regulation EUGDPR PrivacyPrivazy according to plan. http://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm. (2017). (Accessed on 2/2/2018).
6. 2017. Key Changes with the General Data Protection Regulation. (2017). https://www.eugdpr.org/the-regulation.html Accessed:2018-02-01.
7. 2018. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. (2018).
8. Jan Philipp Albrecht. 2016. How the GDPR Will Change the World. *Eur. Data Prot. L. Rev.* 2 (2016), 287.
9. Ann Cavoukian and Alex Stoianov. 2007. *Biometric encryption: A positive-sum technology that achieves strong authentication, security and privacy*. Information and Privacy Commissioner, Ontario.
10. Virtru Corporation. 2008. Email Encryption and Data Security for Business Privacy Virtru. https://www.virtru.com/. (2008). (Accessed on 3/2/2018).
11. Salah Addin ElShekeil and Saran Laoyookhong. 2017. GDPR Privacy by Design. (2017).
12. International Association for Privacy Professionals (IAPP). 2017. 2017 Privacy Tech Vendor Report. https://iapp.org/media/pdf/resource_center/Tech-Vendor-Directory-1.4.1-electronic.pdf. (2017). (Accessed on 3/2/2018).
13. iCONX Solutions Ltd. 2017. GDPR by WIZUDA Wizuda. https://wizuda.com/gdpr/. (2017). (Accessed on 3/2/2018).
14. Roslyn Layton and Edmond Baranes. 2017. GDPR: Short Run Outputs vs. Long Term Welfare. Mapping the EU's General Data Protection Regulation to Best Practices for Online Privacy. (2017).
15. KnowNow-Information Limited. 2016. Consent Management Tool Consentua. http://www.consentua.com/. (2016). (Accessed on 3/2/2018).
16. Baycloud Systems Ltd. 2016. Baycloud DoNotTrack. https://baycloud.com/. (2016). (Accessed on 3/2/2018).
17. MyLife Digital Ltd. 2017. Consentric One Place for Personal Information Management. https://consentric.io/. (2017). (Accessed on 3/2/2018).
18. LLC OneTrust. 2001. OneTrust Privacy Management Software. https://onetrust.com/. (2001). (Accessed on 3/2/2018).