GDPR Compliance: Implementation Use Cases for User Data Privacy in News Media Industry

Ahmedur Rahman Shovon*, Shanto Roy†, Arnab Kumar Shil‡, and Tanjila Atik§
Institute of IT*†§, Department of CSE‡, Jahangirnagar University, BD
Department of CSE†,Green University of Bangladesh, BD
Department of CSE§, Daffodil International University, BD
Cefalo Bangladesh Limited*‡, BD
Email: shovon.sylhet*@gmail.com, shantoroy†@ieee.org, me‡@ruddra.com, tanjila.tanji15§@gmail.com

***Abstract*—The paper presents implementation use cases towards the consequences of maintaining user data privacy after the adoption of GDPR; specifically in the news media industry. General data privacy regulation (GDPR) is a European Union general data protection regulation adopted in 2016 subjected to protect personal data of the citizens in the EU. Besides, it implies to particular restrictions and obligations for handling user data by different companies or organizations. However, although the rule is applicable only if EU citizens are involved, all the companies started adopting the preparation and practice to maintain compliance with GDPR. In this paper, we identify and present the system design and implementation use cases for the news media industry that is compliant with the new regulations. The use cases indicate and explain significant transformation required in user data management process according to the GDPR.**

Keywords- General Data Protection Regulation, GDPR and Compliance, Privacy/Policy by design

I. Introduction

In order to restrict the use of user data by media or service industry, General Data Policy Regulation (GDPR) has been introduced. GDPR defines some particular data usage policies based on certain criteria that must be fulfilled by the developers so that a system preserves it's user rights. GDPR came in front with a view to solving the issue regarding user data misuse without the consent of unaware European Union citizens. However, as every system has worldwide user access including EU citizens, all companies had to change their user data access policies across the world to follow GDPR compliance.

News media industries generally partake various user information by selling subscriptions to a wide range of users. Therefore, it raises the question of how they are managing all these data and using further for advertisement or latter analytics purpose. Now, GDPR is compelling the industry to expose how they are managing all the user data so that the whole process of reusing data remains transparent to users. In addition to that, while mailing offers or showing adds, they have to act carefully in order to avoid user's right violation.

As the data collection and maintenance depend on the user consent, there should be a proper way to communicate between the industry and user's end through an easy to access user dashboard. Applications require to be developed keeping in mind that users should be aware of where, when and how their data is collected and used for further analytics purposes.

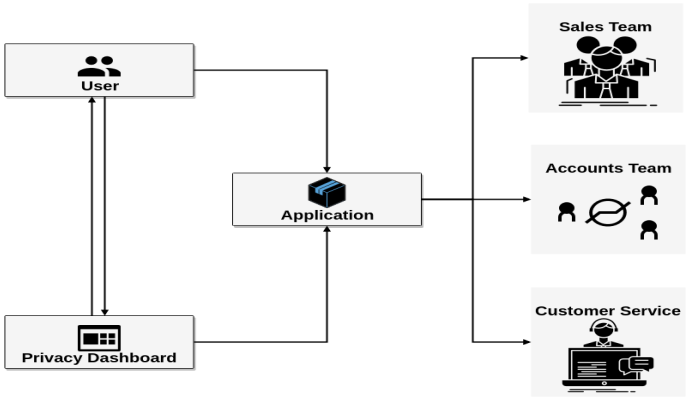

Fig. 1. Privacy by design and GDPR

Therefore, the industries end up enforcing transparent data usage policies that require user permission to use the data for future analysis. This also ensures that if the owner of data or user wants to delete his information, the industries will be responsible to erase that particular data entirely from their database. This is how GDPR is leading towards a policy/privacy by design solution that comes with options towards users for better accessibility, understandings, and management of their owned data. A simple policy/privacy by design with GDPR compliance is shown in **Figure 1**.

In this paper, we designed and developed a model framework that describes the initiation of a user dashboard. The dashboard is a better media of communication and understanding between the industry and the users. Users can read the policies provided by the company and therefore assign the data access rights through their consents. In addition to that, we provided the implementation use cases in the news media industry. We also identified the required transformation of the present system to meet the GDPR compliance.

The rest of the paper is as follows: **Section II** presents the issues and summary guidelines of GDPR compliance. **Section III** identifies and summarizes the implementation use cases of GDPR compliance. Then **Section IV** presents the design and workflow of the news media industry system followed by the consequence discussion in **Section V** and a few related work summaries in **Section VI**.

II. Background and rationale

A. Principle rules of GDPR

There are primarily six principles related to data subject rights that comprise breach notification (Article 33) [1], right to access (Article 15) [2], right to be forgotten (Article 17) [3], data portability (article 20) [4], privacy by design (Article 25) [5] and data protection officer (Article 39) [6]. The principles basically describes the rights a data subject should have on basis of new regulations. Therefore, if there is a data breach the owner of data must be notified as soon as possible. Data subject will need to have the right to know whether or not his particular portion of data is being used for any purpose; and somehow if he wants to erase his previous data, processor or service provider will not be able to store that information further. Another aspect is, the introducing of data portability where the data subject can move or transmit his data from one data controller to another. Privacy by design is not a jargon anymore, it is being applied to different sectors including big data analysis [7] to crisis management using social media [8]. Considering the regulations, controllers need to minimize the amount of data by deducting additional data as well as restricting the use of personal data during data processing (Article 23) [9]. In addition, controllers need to notify the data processing activities along with the local data protection act (DPA) in order to grab approval from the authority.

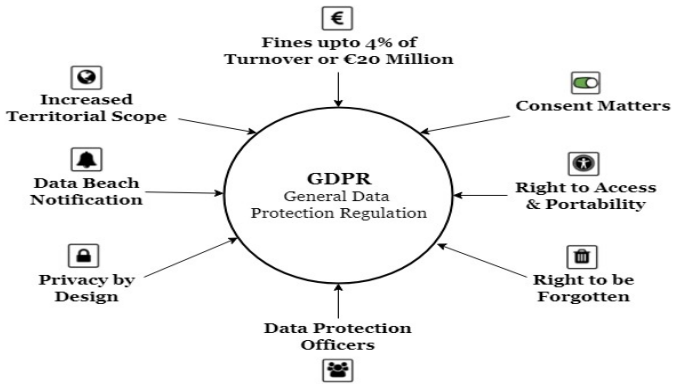

Fig. 2. General Overview of GDPR

Therefore, considering the rights of the data subject, controller or service providers have to perform minimum changes in their user policies and interfaces. Prior to the rules, in privacy program management (PPM) and privacy enterprise management (PEM), system engineering used to exclude consideration regarding user's data behavior. GDPR changed the view and directed it towards more data subject centric decisions to ensure privacy and protection for personal data.

B. Personal data protection

GDPR introduces the protection of data in personal level in the updated regulation policies applicable for only European Union citizens.

C. User consent centric Privacy by Design

Another principle introduced by GDPR is the privacy by design. It refers to the incorporation of the privacy practices from the initial design to the final specification of a system [10]. Privacy by default means that strict privacy settings will be automatically applied upon running or using the system for the first time. GDPR further emphasizes to provide enough protection mechanisms while the personal data of EU citizens is transferred to other countries and requires both a data controller and processor to take the liability.

D. Adoption to the new regulations

GDPR has far more influences over the policies and user experiences beyond regional boundaries. Although the rules are applied for ensuring the data protection across Europe, companies, and service providers have been taking initiatives to amend all the user policies as giant companies like Facebook and Google gave their commitment [11] [12]. But do every company need to take initiative for that? The answer is 'no'. The very first question that comes before deciding is whether or not the company sell products to individuals. Another question is whether or not the company keeps or collects personal data. If the answer to any between these two questions is- yes, the company need to measure whether their clients are from the EU or not. If the potential client is from the EU, the company must follow the regulations to avoid punishments. Since people across the world access to the news pages throughout the day, they register to access news articles and pay for subscription along with providing personal sensitive data. Therefore, news media must adopt the GDPR to establish synchronized user policies all over the world. While adopting, there are several things to keep in mind that include educating employees about the rules, revising user policies, reviewing personal data consent requests, managing and securing data, implementing privacy by design for data, performing data protection by hiring an officer, analyzing third-party risks, etc.

According to the new GDPR, users must have been informed about all the data practices to be done with their personal data. Also, users must have the opportunity to hold their right to give and at the same time to withheld their consent if they disagree to any of the usages of their personal data [13]. However, most of the time the privacy policies are written in an unclear and complicated way [14] and because of the policies being too long, users find it difficult and are unwilling to read the whole content [15].

GDPR aims to improve transparency [16] in terms of the information collected from the data subjects and encourages the use of visualization along with the requirement for using clear and simple language (Art 58, GDPR). To get compliant to this legislation, lately, the Usable Privacy Policy Project [17] in the US has given a try to represent the policy notices in a machine-readable way to display the relevant content in a more user-friendly manner.

Another important issue is to assess the users whether they have understood everything they read on the privacy notice

or not. In this paper distinct concepts of GDPR are discussed and which information must be given to the users while getting consent are extracted. Furthermore, a comparison was made with the old data protection directive 95/46/EC [18].

Some approaches are suggested here related to the notice:

- Firstly, all the data practices and their implementation procedures must be provided.
- A demo approach on how to read the document step by step can be included.
- Different colors and fonts can be used for different topics to keep the users attention.
- For critical legal notations, hyperlinks and pop-up windows can be provided containing illustration and examples related to those notations. These can be accomplished by using Akoma Ntoso mark-up.
- For assessing the proper understanding of the policies by the users, a consent form can be designed where clickable icons can be used to gather explicit consent.
- After taking the consent, same icon can be presented to the users and asked to connect different given icons according to its meaning.

This approach can seem to be annoying thus, needs to be refined further and tested on different categories of users.

III. Implementation use cases

According to the statement of [19], privacy is breached when personal information is available outdoor its supposed context. [20] prescribed some approaches to maintain privacy by utilizing data minimization which may limit the data controllers task of processing and collecting personal data. Giving users control over their own personal data to decide who they want to share those data and in what condition, can strengthen their privacy protection.

The natural persons whose personal data(PD) is processed by a processor or controller are identified as data subject(DS). GDPR compliant system should ensure the rights of Data Subjects(DS) which includes:

- **Right to be informed**: Provide the information listed in Art. 13 [13] if the personal data is supplied by data user. Otherwise, provide information listed in Art. 14 [13].
- **Access right**: Provide access to personal data and information listed in Article 15 [2].
- **Rectification right**: Allow rectification of incorrect personal data and the provision of supplementary data.
- **Right to be forgotten**: Allow erasing personal data when requested. Once deleted it should not be retained.
- **Right to restriction of processing**: Restrain processing of personal data under the situation stated in Art. 18 [21].
- **Notification obligation**: Notify any rectification or erasure or restriction of processing to each recipient stated in Art. 19 [22].
- **Right to data portability**: Allow data subject to transfer personal data as required to another data controller providing that Article 20(1) [4] is applicable.
- **Right to object**: Provide the option to object the processing if the conditions in Article 21 [23] apply. Respond and demonstrate legitimate grounds at earliest convenience.
- **Automated decision making**: Avoid taking decision merely on automated processing including profiling which produces legal effects Article 22 [24].

[25] show an effective methodology for analyzing privacy threats essentially aims on the basic privacy concepts such as non-repudiation, information disclosure, policy content awareness etc. It gives the engineers an initial knowledge about how an intruder might attack a system and helps them setting up effective safeguards while implementing the system.

The primary implementation approaches are as follows:

1) Appoint a data protection officer
2) Stick to a code of conduct
3) Acquire consent for data
4) Ensure 3rd party data processing is compliant to user consent
5) Provide set of policies to end users
6) Develop a dashboard where user can update the consent according to each policies
7) Categorize sources of personal data
8) Protect data subject right to erasure of personal data
9) Establish anonymized processes
10) Establish governance programs
11) Access restriction to approved processes

Our proposed implementation provides GDPR compliance in the following areas:

- Systems and data auditing
- Data maintenance
- Work-flows and data processing
- Policy dashboard configuration
- User consent preference
- User subscription management
- User personal data capture

IV. System Design and Development

User interface (UI) and user experience (UX) design require a user dashboard through which a user can easily gain access to the privacy related options and gives consent for further use of his data. The following paragraphs discusses the user dashboard requirements and functionalities that are required for privacy by design approach. Therefore, the whole management workflow of the news media industry is elaborated followed by the database design issue and miscellaneous.

A. System design for News Media Industry

In order to design a sustainable system with GDPR compliance, we needed to follow the primary implementation approaches mentioned in **Section III**. Therefore at first we identified the required interactions between the user and the system through the user dashboard and added contents for user consent according to that. A web media system basically contains advertisements, data analytics module, cookies, and the site contents- which is generally accessible to users after

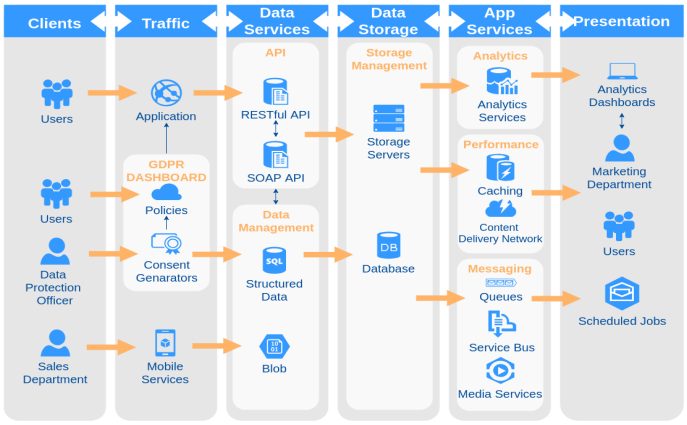

Fig. 3. System Architecture

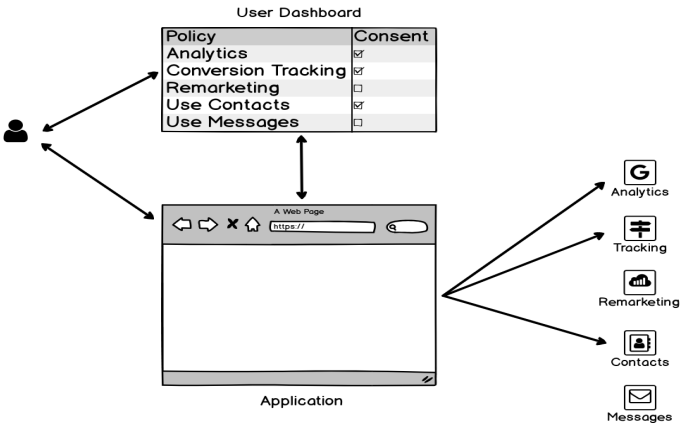

Fig. 4. Dashboard Functions

certain authentication process for users. Except those, the news media website also contains free site contents, newsletter, and other payment oriented monetary modules. The additional part here indicates the policy dashboard for users where user can put his preferences from which the system learns how to handle user data. As the owner of the data, it is completely up to the user whether or not the system can use his data for further analytics or business processes. According to the user consent input, the system stores the privacy data in an access control system through which other analytics module have permission or not to use user data in later cases. The design issues and processes are presented in **Figure 3**.

B. Dashboard Requirement and Functionalities

The user dashboard is the primary concern for the industry as it is the communication and understanding media for them with the users. The dashboard should include the user data policies along with the form that presents user consent options. The application checks initially the user preferences and then acts accordingly. For example, if the user gives his consent to use his data for only 2 options among 5 options, then the application will collect only those data and pass to other analytical machines for further use or analysis. In **Figure 4**, there are five policies for a user including analytics, conversation tracking, remarketing, use contacts, and use messages. A general user has given his consent for only analytics, conversation tracking, and contacts by ticking on the checkmark. Now the application collects data from the user accordingly and lets the data pass to other engines accordingly. Point to be noted that the system will also be responsible to convey the message towards the user on how his data is being used.

The user dashboard is required to have the following functionalities in general:

- Add or delete policies as needed for the application
- User can Check/Uncheck per policy (Give Consents)
- User can See and Update Consents in a dashboard

C. News media management workflow

Data management workflow for a news media includes from the data collection through application according to the user consents to the data transferring gateway to other applications. The application is always responsible for tracking any change that user dashboard provides and collecting the user data. Then the data is stored privately in secure storage lied in their own data centers according to various categories. Later the stored data is passed to other applications for further processing through privacy dashboard. **Figure 5** represents the data flow in a particular system.

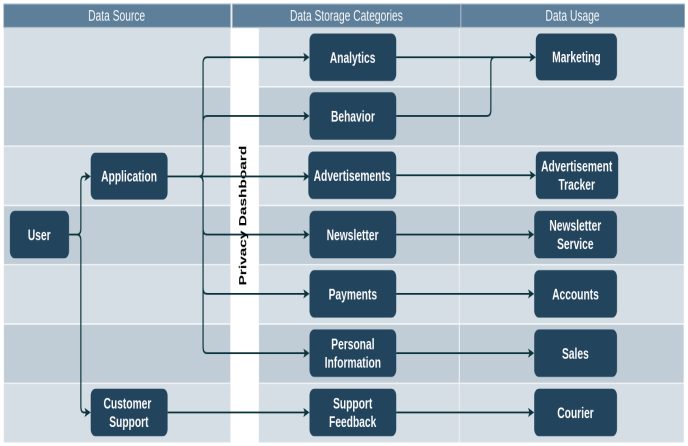

Fig. 5. News Media Corporation Data flow

D. Sample User Dashboard

A standard user dashboard contains the data usability policies and related options to users requesting for their permission in re-usability of user created contents. **Figure 6** represents a sample parallel user dashboard that is easily accessible to users. After reading the company policies, users become able to make the changes in remarketing and recommendation use cases that enforces credibility towards the reuse of user data.

The dashboard expresses whether or not a user is interested in receiving offers from the company through mail or phone. Also as the owner or creator of data, user is able to recommend whether the company will be able to use user data for future customer experience or for enabling personalized advertising

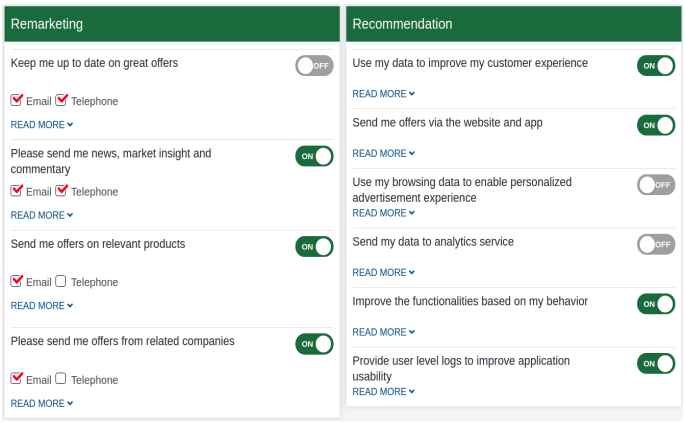

Fig. 6. Sample User Dashboard

experiences. Whether other third parties will be able to use data for behavior analysis or other analytic services- options are present within the dashboard for user permission as well.

V. Discussion

A. Penalty

[26] analyzes how the EUs GDPR will affect the IoT firms in terms of legal and preventive cost all over the world which deals with huge amount of personal information. According to the reference given by Ponemon Institute in 2016 [27], four personal data breach cases out of around twenty four thousands were analyzed to compare the estimated cost damage before and after GDPR. Assuming the average per capita cost of a data breach over the last four years as $150 and for each violation of GDPR costs 2% of a firms global turnover, the results of the analysis shows that in some cases a firms cost may be increased 3-18 times than before GDPR is applied based on the annual turnover of any firm for the past year. Vizio, an electronic product development company was charged with a $2.2 million fine after using content-aware apps to track user data without permission. The data of the users was collected intending to analyze personal TV habits info. If it would happen in current time with GDPR enforced, it would have been $292 million, more than hundred times larger penalty. In addition to that, users have full right to demand compensation for damages if experienced any material or non-material damage due to a violation of GDPR rules.

B. Liabilities of both service provider and consumer

Maintaining proper data privacy requires both parties to be aware of the data usage policies and regulations. Liability goes to both parties as users are responsible for getting familiar with the policies and put ticks on their preferable choices of data usage. On the other hand, service providers must follow user's preference and use data for further purpose thereby.

C. Issues

GDPR has several issues though. [28] enlightens some problems that can be caused when the new GDPR will be in force. The information flow within the digital market can be scattered because of the uneven national provisions. It will be infeasible for a cloud provider to have prior written consent from all of its data subjects before starting any processing task. Furthermore, to ensure highest level of security in every processing the CPs must carry out security assessments more frequently increasing the cost in a considerable amount and eventually the customers will have to bear that cost.

Also, cloud providers must optimize operational cost by adopting efficient privacy compliant practices while handling the data [29] as any information which can identify an individual including name, location, ID number, genetic, and biometric data etc. are considered as personal data.

VI. Related Works

In [28], the major changes in the new GDPR in cloud environment relating the field of healthcare are discussed. Much significance is given on the role of data controller and data processors in the GDPR and also their roles have been refined in some extent. The data subjects are now given more privileges which in turn increases the responsibilities of data controllers. A data controller must find a trustful processor that will maintain the compliance with the new principles such as the right for data access, data portability and also to be forgotten. To maintain appropriate security, both the controller and the data processor have to evaluate the risks associated with the processing of personal data and take feasible measures to eradicate those risks.

[30] focused to solve these problems by introducing the use of some widely used icon sets while preparing the privacy policy to facilitate the users task of decision making. Having the ability to present the legal information in a much clear, fast and effective way, graphical elements such as images icons etc. can improve the readers understanding capability.

The primary focus in [31] is to create a supportive environment for health and social care sectors and an analysis of the impact and related changes to the Information Governance Toolkit (IGTK) in the primary care sector in England considering the presence of new GDPR which will replace the UK data protection act,1998. The paper also describes the impact of introducing cloud computing in e-health, different risk factors and the maintenance of the security in the cloud. 8 principles of the data protection act,1998 are summarized and core 5 elements of information governance are discussed. [32] identified three major threats to security, that is tampering with data (Integrity), loss of data(availability), and unauthorized access to data (confidentiality). With these three under consideration, the risk of data security will be minimized.

The new GDPR that is in force from 25 May,2018; has imposed more obligations to regulate the privacy issue while collecting, storing and processing the personal data of EU citizens [16]. This paper aims at capturing the privacy requirements introduced by GDPR and providing general guidance to the engineers for developing GDPR-standard software. This paper further gave an overview on the roles and responsibilities of the liable authorities while developing a GDPR compliant

system via UML use-case diagrams. While implementing privacy policies within an organization several factors are too be considered such as directives, inspections, fine amount, and other profit and loss side effects [33].

VII. Conclusion

The primary concern of GDPR is to protect user personal data by enforcing the law. These days, all companies including Google, Facebook, and Amazon etc are following the rules and regulations. The news media industry is still adopting the new framework towards more user aware data usage policies. Processing of data is now more transparent towards users end. As the owner of data, users can change their preference at any time and become more aware of the policies on where and how the data is being used by other applications. This leads to privacy or policy by design that is more concerned about the security of personal data. Our paper discussed the design and developmental adoption to the new rules and regulations. Furthermore, we discussed the user dashboard in details so that other companies can follow the adoption with framework transformations that comply with the new regulations.

Acknowledgement

The work has been partially funded by Green University Research Fund.

References

[1] "Article 33 eu general data protection regulation (eu-gdpr). privacy/privazy according to plan." http://www.privacy-regulation.eu/en/article-33-notification-of-a-personal-data-breach-to-the-supervisory-authority-GDPR.htm, (Accessed on 07/29/2018).

[2] "Article 15 eu general data protection regulation (eu-gdpr). privacy/privazy according to plan." http://www.privacy-regulation.eu/en/article-15-right-of-access-by-the-data-subject-GDPR.htm, (Accessed on 07/29/2018).

[3] "Article 17 eu general data protection regulation (eu-gdpr). privacy/privazy according to plan." http://www.privacy-regulation.eu/en/article-17-right-to-erasure-'right-to-be-forgotten'-GDPR.htm, (Accessed on 07/29/2018).

[4] "Article 20 eu general data protection regulation (eu-gdpr). privacy/privazy according to plan." http://www.privacy-regulation.eu/en/article-20-right-to-data-portability-GDPR.htm, (Accessed on 07/29/2018).

[5] "Article 25 eu general data protection regulation (eu-gdpr). privacy/privazy according to plan." http://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm, (Accessed on 07/29/2018).

[6] "Article 39 eu general data protection regulation (eu-gdpr). privacy/privazy according to plan." http://www.privacy-regulation.eu/en/article-39-tasks-of-the-data-protection-officer-GDPR.htm, (Accessed on 07/29/2018).

[7] G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y.-A. de Montjoye, and A. Bourka, "Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics," *arXiv preprint arXiv:1512.06000*, 2015.

[8] K. Boersma, P. Meier, and M. Imran, "The use of social media for crisis management: a privacy by design approach," in *Big Data, Surveillance and Crisis Management*. Routledge, 2017, pp. 33–51.

[9] "Article 23 eu general data protection regulation (eu-gdpr). privacy/privazy according to plan." http://www.privacy-regulation.eu/en/article-23-restrictions-GDPR.htm, (Accessed on 07/29/2018).

[10] S. Gürses, C. Troncoso, and C. Diaz, "Engineering privacy by design," 2011.

[11] "Facebook's commitment to data protection and privacy in compliance with the gdpr — facebook business," https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr, (Accessed on 07/29/2018).

[12] "General data protection regulation (gdpr) — google cloud," https://cloud.google.com/security/gdpr/, (Accessed on 07/29/2018).

[13] P. O. P. DATA, "Article 29 data protection working party," 2012.

[14] E. Commission, "Special eurobarometer 431: Data protection," 2015.

[15] F. Schaub, R. Balebako, A. L. Durity, and L. F. Cranor, "A design space for effective privacy notices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 1–17.

[16] G. D. P. Regulation, "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," *Official Journal of the European Union (OJ)*, vol. 59, no. 1-88, p. 294, 2016.

[17] N. Sadeh, A. Acquisti, T. D. Breaux, L. F. Cranor, A. M. McDonald, J. R. Reidenberg, N. A. Smith, F. Liu, N. C. Russell, F. Schaub *et al.*, "The usable privacy policy project," Technical report, Technical Report, CMU-ISR-13-119, Carnegie Mellon University, Tech. Rep., 2013.

[18] E. 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," *Official Journal of the EC*, vol. 23, no. 6, 1995.

[19] H. Nissenbaum, "Privacy as contextual integrity," *Wash. L. Rev.*, vol. 79, p. 119, 2004.

[20] K. Borcea-Pfitzmann, A. Pfitzmann, and M. Berg, "Privacy 3.0:= data minimization+ user control+ contextual integrity," *IT-Information Technology Methoden und Innovative Anwendungen der Informatik und Informationstechnik*, vol. 53, no. 1, pp. 34–40, 2011.

[21] "18. right to restriction of processing - easygdpr," https://easygdpr.eu/gdpr-article/18/, (Accessed on 02/05/2019).

[22] "19. notification obligation regarding rectification or erasure of personal data or restriction of processing - easygdpr," https://easygdpr.eu/gdpr-article/19/, (Accessed on 02/05/2019).

[23] "21. right to object - easygdpr," https://easygdpr.eu/gdpr-article/21/, (Accessed on 02/05/2019).

[24] "22. automated individual decision-making, including profiling - easygdpr," https://easygdpr.eu/gdpr-article/22/, (Accessed on 02/05/2019).

[25] K. Wuyts, R. Scandariato, and W. Joosen, "Empirical evaluation of a privacy-focused threat modeling methodology," *Journal of Systems and Software*, vol. 96, pp. 122–138, oct 2014. [Online]. Available: https://doi.org/10.1016/j.jss.2014.05.075

[26] J. Seo, K. Kim, M. Park, M. Park, and K. Lee, "An analysis of economic impact on iot under gdpr," in *Information and Communication Technology Convergence (ICTC), 2017 International Conference on*. IEEE, 2017, pp. 879–881.

[27] "2017 cost of data breach study: United states," https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states, (Accessed on 08/25/2018).

[28] R. Ducato, "Cloud computing for s-health and the data protection challenge: Getting ready for the general data protection regulation," in *Smart Cities Conference (ISC2), 2016 IEEE International*. IEEE, 2016, pp. 1–4.

[29] P. Blume, "It is time for tomorrow:: Eu data protection reform and the internet," *Journal of Internet law*, vol. 18, no. 8, pp. 3–13, 2015.

[30] A. Rossi and M. Palmirani, "A visualization approach for adaptive consent in the european data protection framework," in *E-Democracy and Open Government (CeDEM), 2017 Conference for*. IEEE, 2017, pp. 159–170.

[31] I. N. Shu and H. Jahankhani, "The impact of the new european general data protection regulation (gdpr) on the information governance toolkit in health and social care with special reference to primary care in england," in *2017 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 2017, pp. 31–37.

[32] I. de la Torre Díez, K. Saleem, S. G. Alonso, M. S. Khalil, S. Hamrioui, J. J. Rodrigues, and M. L. Coronado, "Requisites of security, reliability and usability in 2 mhealth apps: Systematic analysis and proposed 3 architecture 4," 2018.

[33] M. J. Culnan and C. C. Williams, "How ethics can enhance organizational privacy: lessons from the choicepoint and tjx data breaches," *Mis Quarterly*, pp. 673–687, 2009.