Guidelines for GDPR Compliant Consent and Data Management Model in ICT Businesses

Dijana Peras
Faculty of Organization and Informatics
University of Zagreb
Department of Information Systems Development
Pavlinska 2, 42000 Varaždin, Croatia
dijana.peras@foi.hr

Abstract. *The purpose of this paper is to set guidelines for managing consent and personal data in ICT businesses taking into account the provisions of the General Data Protection Regulation (GDPR). The analysis of previous studies on consent management models and GDPR requirements, as well as the comparison of five data management models was made. Based on the analysis, guidelines for the framework of GDPR compliant Consent and Data Management Model in ICT businesses were proposed. The result of the study can help data controllers to improve the integration of consent and data management and to demonstrate compliance with GDPR.*

Keywords. Consent management, data management, GDPR, informed consent, framework of consent

1 Introduction

According to the General Data Protection Regulation (Regulation (EU) 2016/ 679 2016), consent for the processing of personal data for one or more specific purpose is one of six legal basis of lawfulness of processing. It can only be an appropriate lawful basis if user is offered control and a choice with regard to accepting or declining the terms offered or declining them without harm (Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679 2016). However, in practice consent is the most common basis of data processing (Hunton and Williams 2016). GDPR imposes strict rules on obtaining consent on personal data processing, where data controller must be able to proof the validity of consent. Data controllers are expected to be prepared for demonstrating compliance, especially in case they are dealing with various users and using multiple data sources where there are a lot of complexities involved in building and maintaining a complete model of how personal data is used (Fatema et al. 2017). ICT businesses have different approaches on how to deal with consent, and they usually provide limited solutions. Furthermore, complexity in providing consent and expressing privacy preferences can negatively impact data subject's willingness to disclose personal information (Mont et al. 2009). Furthermore, ICT businesses contain a large number of confidential and sensitive data, which should be protected from malicious activities. Therefore, ICT businesses should cover all the areas that represent a security risk Forming a consent model is an important step in ensuring compliance with the GDPR that will help data controllers to meet the requirements related to the specificity and uniqueness of the data.

This paper will identify important concepts of consent, present guidelines for the framework of managing consent in line with GDPR and propose guidelines towards the successful data management model in line with GDPR. It consists from following sections: an introduction is presented in Section 1. Section 2 describes State of the Art. The research method is presented in Section 3. Sections 4 and 5 are focused on identifying important concepts of consent, describing framework for consent management model and components of GDPR compliant data management model for ICT businesses. Conclusions with Future research are presented in Section 6.

2 State of the Art

The concept of consent originated in the field of medicine. In framework for enforcing consent policies for healthcare systems based on workflows, consent had a central role for assigning permissions to subjects that access patients' medical data (Russello, Dong, and Dulay 2008). In biomedical research (Vayena and Blasimme 2017), the notion of control was divided along three dimensions that debate on data protection: control over data access, control over data uses and control through governance. Other report (Coiera 2003) has outlined several possible models (e-Consent) for determining that patient consent exists prior to

allowing access to health information, which will contain the specific conditions under which the data to which it is attached can be retrieved. Electronic consent (Rowan et al. 2017) was also explored on a Health Social Network to improve the form and accessibility of information presented to users. This study suggested returning control over private health information back to the users, in line with the GDPR. The outline of a new model for informed consent used for personal genome testing, which can meet the norm of providing sufficient information and the norm of providing understandable information, was presented by Bunnik et al. (Bunnik, Janssens, and Schermer 2014). The CMA framework described by Hyysalo et al. provided a simple, general purpose consent management framework and architecture that conforms to the GDPR, with main focus on consent and the use of consent for enabling secure transactions, for authorizing data access to services and for health-related personal data management and processing (Hyysalo et al., 2016).

In order to examine the use of consent in an online environment, where the individuals are able to control the collection, use and dissemination of their personal data, researchers have adopted Faden's and Beauchamp's theory of informed consent (Agrafiotis, 2012). Conceptual model of informed consent based on disclosure, comprehension, voluntariness, competence and agreement was provided (Friedman, Felten, and Millett 2000), which examined how these components play out in a wide range of online interactions. Another model for organizations (Mont et al. 2009), enabling capturing consent, managing and enforcing it, along with revocation, included a set of basic requirements of relevance for organizations: Personal Consent & Revocation Assistant, Data Registry, Consent and Revocation Provisioning, Privacy-aware Policy Enforcement, Disclosure and Notification Manager, Audit and Risk Assurance. Furthermore, authors (Karjoth, Schunter, and Waidner 2003) described the Platform for Enterprise Privacy Practices (E-P3P), which defined technology for privacy-enabled data management and introduced separation of duty between the privacy officer, the security officer and the customers. Architecture for a privacy-enhanced database management system was described and algorithms for privacy constraint processing were discussed (Thuraisingham 2005). Bertino et al. discussed requirements towards the development of privacy-preserving database management systems (Bertino, Byun, and Li 2005), who presented two initial solutions dealing with purpose meta-data and their use in access control. Informed consent online was assessed according to set criteria, and it was examined how cookie technology and Web browser designs have responded to concerns about informed consent (Millett et al., 2001). The rule types, which are the essence of consent model and enable the expression of actions associated with obtaining and revoking consent for the use of personal data, were analyzed (Casassa Mont et al., 2011). Consent management model resulting from the focus group sessions with experts in the field of privacy and consent described three main categories for which it is necessary to require consent (Agrafiotis, 2012): collection of personal data, use of personal data and sharing of personal data. MyData was designed as a framework and model for a user-centric approach for managing and processing personal information in the context of online services (Rissanen, n.d.). A provable expression of consent available for aggregated personal data was offered in a form that allows passing it on, that can be retained, and that remains verifiable by third-parties (Pöhls, 2008). Finally, consent and data management model (Fatema et al., 2017) addressed the lifecycles of consent and data along with the various interactions between their stages and between consent and data lifecycle states due to change of context.

3 Research method

This paper aims to set guidelines for managing consent and personal data in ICT businesses taking into account the provisions of the GDPR. For the purpose of defining framework of GDPR compliant consent management, important concepts of consent were defined. The analysis of previous studies on consent management models and GDPR requirements was made, which resulted with general guidelines for obtaining the consent and processing personal data in line with GDPR.

The comparative analysis of five data management models proposed by Thuraisingham, Mont et al., Rissanen, Hyysalo et al. and Fatema et al. was made. Models were compared based on their elements and components. The presence of the following elements was examined: a) legal basis for personal data processing, b) data controller, c) data subject, d) control through governance, e) data processes, f) privacy levels, g) authorization, h) foundation, i) policy layers, j) policy rules, k) possibility of consent revocation, l) context dependency, and m) validity checking. Elements of Consent and Data Management Models are listed in Table 1. Models were further examined based on described data management model components. Collected type of information was listed for each consent management model, and in case the model did not collect examined information, the n/a mark was assigned. Based on their functions, data management model components were grouped into five units: Contact Interface, Consent Management, Data Management, Origin Management and Context Management. Components of Consent and Data Management Models are listed in Table 2.

Guidelines for the framework of GDPR compliant consent management were then used to describe those data management model units. Furthermore, a scenario of obtaining consent for processing personal data for the marketing purposes in ICT businesses was created.

Table 1. Elements of Consent and Data Management Models

	Thuraisingham Model	**Mont et al. Model**	**Rissanen Model**	**Hyysalo et al. Model**	**Fatema et al. Model**
Legal basis	consent	consent	consent	consent	consent
Data controller	privacy controller	organization	operators	operators	organization
Data subject	users	data subjects	user	account owners	user
Control through governance	governments	regulators	n/a	n/a	n/a
Data processes	collect, process, store, share, delete/modify	collect, process, store, share, delete/modify	collect, move and process	protection, authorization, control	collect, use, store, archive, share, delete
Privacy levels	public, private, or highly private	n/a	n/a	n/a	consent permissions, obligations and validity
Authorization	required	required	required	required	required
Foundation	privacy policy	privacy policy	predefined rules and policies	privacy policy	access control policy, participants policies, GDPR
Policy layers	n/a	legal, business, process, application, information, system, network	n/a	n/a	n/a
Policy rules	n/a	notification, access control, update, protection, obligation	n/a	n/a	n/a
Consent revocation	n/a	yes	yes	yes	yes
Context dependency	yes	yes	yes	yes	yes
Validity checking	no	no	yes	yes	yes

Table 2. Components of Consent and Data Management Models

	Thuraisingham Model	**Mont et al. Model**	**Rissanen Model**	**Hyysalo et al. Model**	**Fatema et al. Model**
Contact Interface	User Interface	Personal Consent & Revocation Assistant	Single Point of Contact	Data Account	User Interaction Handler
Consent Management	Constraint Manager	Privacy-aware Policy Enforcement	Data Sources	Data Source	Consent Manager
Data Management	DBMS and Database Design Tool	Data Registry, Risk Assurance, Disclosure and Notification Mng.	Data Sinks that use personal data	Data Sink	Data Manager
Origin Management	n/a	Audit	n/a	n/a	Provenance Manager
Context Management	Query Processor and Update Processor	Consent and Revocation Provisioning	n/a	n/a	Context Handler

4 Guidelines for the framework of GDPR compliant consent management

This chapter will focus on identifying the important concepts of consent, as well as on requirements for the framework of consent management.

4.1 Concepts of consent

According to the analyzed models (Thuraisingham 2005) (Millett, Friedman, and Felten 2001) (Casassa Mont et al. 2011) (Rissanen n.d.) (Fatema et al. 2017), the structure of the consent can generally be described as follows:

a) consent form, filled by data subject or his representative,
b) context of a consent, which usually contains data about time, location and relevant information communicated between data subjects and data controllers, and which can be modified by data controller, data subject or environment,
c) permissions set by data subject, such as the validity period, allowed party, data format and category, prohibited and permitted actions and their purpose, as well as the conditions for given permissions, if they exist, and obligations that result in certain activity or event.

Furthermore, five conceptual components of consent were detected (Friedman et al., 2000): disclosure, comprehension, voluntariness, competence and agreement. This means that the data subject should know the purpose and benefits of disclosure, as well as potential harms. He should be able to interpret accurately Terms of Use, Privacy Statement and purpose of data processing, as well as the consent form through which the consent is being obtained. However, there is no guarantee that all data subjects will completely understand all aspects of the consent. Voluntariness means that the data subject is not forced or manipulated to give a consent. Data subject has to be mentally and physical competent to give the consent. People who lack those competences (e.g. children under age of 16, mentally ill persons and similar) need to have their representative since they cannot reliably determine the appropriateness of the information they choose to disclose. Agreement means the data subject is given a choice to accept or decline the consent. Furthermore, it means he can choose among different options, and decide to approve or decline them without losing the right to service. He can also choose to withdraw his consent at any time. Stated criteria have to be satisfied in order to obtain the valid consent.

Onwards, the requirements related to consent provided by GDPR (Regulation (EU) 2016/ 679 2016) were collected, and they are as follows:

- consent should be freely given, specific, informed and unambiguous,
- consent should be given by a written or an oral statement,
- consent should cover all processing activities carried out for the same purpose or purposes,
- consent request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided,
- the principles of fair and transparent processing require that the data subject is informed of the existence of the processing operation and its purposes,
- the data subject shall have free choice and be able to refuse or withdraw consent,
- protection of personal data requires setting out of the rights of data subjects and the obligations of those who process personal data,
- modalities should be provided for facilitating the exercise of the data subject's rights, including mechanisms to request access to and rectification or erasure of personal data,
- the controller shall be able to demonstrate that processing is performed in accordance with GDPR.

4.2 Framework of Consent Management

Stated structure of consent, conceptual components of consent and GDPR requirements for obtaining the consent and processing personal data are the foundation of the proposed framework of consent management. Guidelines for the framework of consent management are listed in Table 3.

Table 3. Guidelines for the framework of GDPR compliant consent management

	Guidelines
1	The rights, responsibilities and obligations of data subjects, data controllers and allowed party should be identified.
2	The consent management modalities required for data processing should be defined.
3	Modalities for consent withdrawal should be provided.
4	Capability to adapt to changes of law and privacy policy requirements should be provided.
5	Transparent processing of personal data should be possible.
6	Data erasure should be enabled.
7	Data portability should be possible.
8	Data subject should be able to manage his personal data.
9	Privacy Policy should be understandable.
10	Appropriate technical and organizational measures shall be implemented to demonstrate that processing is performed in accordance with GDPR.

Guidelines for the framework of consent management listed in Table 3. were used to describe the data management model according to GDPR principles for ICT businesses. Thus, in the following chapter, harmonization of data management model according to GDPR principles will be presented.

5 Guidelines for GDPR Compliant Data Management Model

The structure of proposed model is based on the detected components of data management models stated in chapter 3, and amended with guidelines for the framework of GDPR compliant consent management defined in chapter 4. It is structurally most similar to the data management model defined by Fatema et al.

5.1 Components of Data Management Model

To meet the guidelines set out in Table 3, proposed data management model should consist of following five components:

Contact Interface. This component supports interaction between data controllers and data subjects, and serves for obtaining consent and exchange of consent related information. It manages all communication between the data subject and the data controller, and assists data subjects in expressing the consent by providing transparent privacy policy. According to Karjoth et al. (Karjoth, Schunter, and Waidner 2003), privacy policy describes what operations for which purpose by which data user can be performed on each personal data, and consists of three elements: a) header with information about privacy policy, b) declarations of policy and c) authorization rules. Declarations of policy consist of:

- data subjects' personal information,
- information about internal and external data users,
- information about purpose of data processing and subsets of the purpose (if applicable), which can be performed in case the main purpose is approved,
- information about data activities, such as collecting, processing, storing, archiving, transferring etc., and
- information on the essential activities used for defining authorization rules.

Contact Interface also handles all data subject actions through unified interface, and helps them to pursue their rights regarding access to personal data, rectification, erasure ('right to be forgotten'), restriction of processing, data portability, object and automated individual decision-making (Regulation (EU) 2016/ 679 2016). These rights refer equally to all data subjects and their application is independent of individual consent.

Consent Management. Consent permissions need to be obtained prior to collecting and processing the data. Consent Management records privacy instructions, including a description of different contexts under which a new consent is required, or conditions under which the data subject needs to be informed. It also records consent permissions related to termination of data processing, consent validity and communication of personal data breach, but stores only information relevant for current data processing. All other information related to context of the consent, but irrelevant for current data processing, are being stored in Origin Management. Before collecting or processing personal data, it is necessary to obtain user's consent through consent form. In order to ensure fair and transparent processing in respect of the data subject, consent form should contain following information (Regulation (EU) 2016/ 679 2016):

1) the identity and the contact details of the data controller and data protection officer,
2) the purposes and the legal basis for the processing,
3) the categories of personal data concerned,
4) the recipients of the personal data (including recipients in a third country or international organization),
5) the period for which the personal data will be stored,
6) the right to access, modify or erase personal data, restrict processing or object to processing, and right to data portability,
7) the right to withdraw consent at any time and to lodge a complaint with a supervisory authority,
8) the existence of automated decision-making, including profiling.

Consent form should clearly state the terms of consent, and it should contain a series of options for which the data subject can, but does not have to give a consent.

Context Management. It manages context, but also detects changes of context and shares them with Consent Management, Data Management and Origin Management. It collects information on modifications made by data controller (e.g. change of the purpose of the processing), data subject (e.g. data modification, consent withdrawal) or environment (e.g. expiration of consent or data, change of partner). It is important to notice the consent is given in a particular context, for a specific purpose. The purpose can change over time, which means the context of the consent will also change and the consent will no longer be valid. Change of Context can be driven by the following events: data modification, consent withdrawal, consent expiry, data breach, business acquisition, change of data processor etc.

Data Management. It handles data according to the given consent and provides personal data protection control (access control, anonymization, pseudonymization etc.). It performs following actions: collecting, processing, sharing (transferring), storing, deleting, archiving. To be able to manage the consent,

it has to know all the locations where data is stored. It also needs to know at any time where the data is located within the organization, the format in which data is stored and the information to whom the data has been disclosed. This component is critical and has to be secured and protected. The concept of control is observed through three dimensions that are related by a causal connection, which means that one control can affect other controls (Vayena and Blasimme 2017):

a) Control over data access is the basis which sets the conditions of data disclosure. Authorization rule specifies activities that may be executed on personal data by the data controller if the data subject has given him a consent for specific purpose. There are two types of authorization rules: authorization rule with a condition and authorization rule without the condition. If the authorization rule contains a condition, it applies only if the condition is met.
b) Control over data uses determinates who has the right to access personal data and the purposes for which personal data is used, and decides on the relevance of the purpose and its compliance with the interests and expectations of the data subject. Control over data uses is responsible for keeping unauthorized persons away from the personal data. If the person who tries to access personal data is not authorized to execute specific task, he will not be allowed to do it. Furthermore, it can limit the access of applications in case their request for accessing certain personal data is denied.
c) Control through governance is related to management structures, including GDPR, in which data subjects are put in the focus and are given back the control over their personal data

Origin Management. It keeps history of all activities related to consent, which could help identify origin and other relevant information in data activities. It records the location of data and tracks the data that were disclosed to third parties. With the introduction of GDPR, its utility will increase, since it is capable to prove whether the data was used in line with the consent. Furthermore, it can track activities related to change of consent, data breach, data modification etc. Its main purpose is to ensure compliance by providing evidence of taking proper actions at critical moments.

Components of GDPR compliant data management model and interactions between them are presented in Figure 1. The following subchapter will describe scenario of obtaining data subject's consent for the purposes of marketing in ICT businesses.

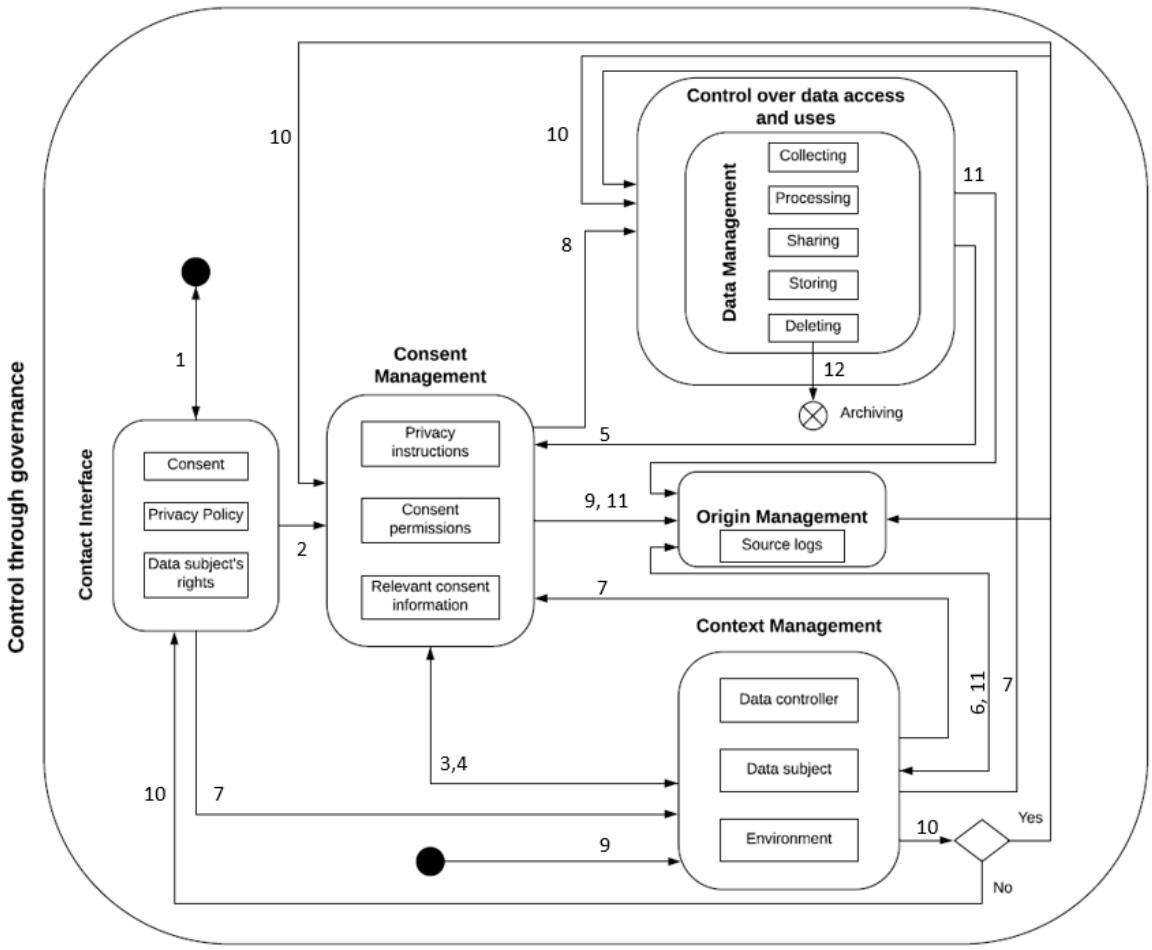

Figure 1. Components of GDPR compliant data management model and interactions between them

5.2 Scenario of obtaining consent for the purposes of marketing

In following scenario of obtaining data subject's consent for the purposes of marketing, which is described in Table 4, data subject can choose whether his data will be used for the purposes of marketing.

Table 4. Scenario of obtaining consent for the purposes of marketing

Scenario of obtaining consent for the purposes of marketing	
1	Data controller seeks data subject's consent for the purposes of marketing through Contact Interface. If the data subject decides to give a consent for the purposes of marketing, he can choose the preferred communication channel(s) of receiving notifications about special offers and novelties. There are multiple options to choose from: e-mail, SMS, telephone, Viber, Skype, Messenger, etc.
2	After the decision is made, the consent is stored in Consent Management. Consent management records the consent by extracting and storing relevant information on consent validity, obligations and permissions.
3	Consent management shares information about consent origin with Origin management and Context Management. Context Management registers the context of the consent.
4	If the data subject withdraws the consent for processing his personal data for the purposes of marketing, the new context is being generated and stored in Context management. Context Management initiates interaction with Data Management, which immediately stops processing and removes all personal data, and Consent Management, which updates the consent accordingly. If the consent validity has expired, Context Management receives notification from the Consent Management.
5	In case the data controller wants to notify data subject about special offers and novelties via Messenger, he first needs to check if he is allowed to do so. Data Management initiates the interaction with Consent management and checks consent permissions before making a decision. It the data subject has given a consent for communication via Messenger, he will receive notifications. If he did not give the consent, data controller can consult Consent Management about other options of notifying data subject (via e-mail, SMS etc.). If data subject has given the consent for receiving notifications via other communication channel, data controller can send him special offers and novelties, but if he didn't give the consent, the notification should not be sent.
6	Origin Management notes changes of context.
7	Data management stores permissions for the intended data processing, which are in line with obtained consent for the purposes of marketing. In case of change of consent permissions by data subject, Contact Interface informs Context Management about the context of changes that have occurred. Context management sends the information to Consent Management and Data Management. Consent Management updates the information on consent permissions to restrict the access to affected data, while Data Management checks the updated consent and accordingly adjusts the data collection process.
8	After it detects the changes of consent, Consent Management updates information related to data processing as mentioned in step 7 and sends new consent to Origin Management and Data Management. Data Management then stops data processing and checks updated permissions for further data processing. If the data subject has given permissions for processing personal data for the purposes of marketing, Data management will execute the task, otherwise it will not.
9	Context Management collects information on modifications made by data controller, data subject or environment.
10	Context Management then checks consent permissions in Consent Management to determine if there is a need to communicate with data subject. If the context of the consent has changed, it initiates interaction with Contact Interface in order to get the new consent from data subject. If there is no need for the new consent, it repeats step 6 and 7.
11	Origin Management keeps history of all activities related to consent, and records the process of obtaining consent from Contact Interface, consent information from Consent management, and all the activities that were using consent from Data management. It keeps track of when the request was received and what changes were performed. Origin Management also keeps records of archived consents as described in Step 7. In case personal data were used for the purposes of marketing before receiving the information on withdrawal of consent, it would be possible to prove the processing was valid at that moment.
12	If the user requires deletion of personal data related to purposes of marketing, Data Management deletes and archives the information, including data and consent origin. In case data subject requests termination of contract with data subject, any personal data that is no longer needed will be destroyed. Data origin and processing activities will be archived, since they are required for demonstrating compliance with GDPR.

6 Conclusions with future research

In this paper, state of the art of consent and data management was presented. Based on the analysis of GDPR requirements and existing data management models, guidelines for managing consent and data in ICT businesses were defined. Important concepts of consent were identified and the guidelines for the framework of consent management were presented. The data management model for ICT businesses, which meets the requirements of GDPR related to the specificity and uniqueness of the data, was proposed. Model was then explained by simple scenario of obtaining consent for the purposes of marketing. Given guidelines can help data controllers to demonstrate compliance with GDPR.

Further work should focus on defining solutions and technologies that could be used to implement the proposed model.

References

Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, (2016). https://iapp.org/media/pdf/resource_center/wp29_consent-12-12-17.pdf, accessed November 4, 2018.

Bertino, Elisa, Ji-Won Byun, and Ninghui Li, (2005). Privacy-Preserving Database Systems. *In* Foundations of Security Analysis and Design III. Alessandro Aldini, Roberto Gorrieri, and Fabio Martinelli, eds. Pp. 178–206. Berlin, Heidelberg: Springer Berlin Heidelberg. http://link.springer.com/10.1007/11554578_6, accessed March 23, 2018.

Bunnik, Eline M., A. Cecile J.W. Janssens, and Maartje H.N. Schermer, (2014). Informed Consent in Direct-to-Consumer Personal Genome Testing: The Outline of A Model between Specific and Generic Consent: Informed Consent in Direct-to-Consumer Personal Genome Testing. Bioethics 28(7): 343–351.

Casassa Mont, Marco, Siani Pearson, Sadie Creese, Michael Goldsmith, and Nick Papanikolaou, (2011). A Conceptual Model for Privacy Policies with Consent and Revocation Requirements. *In* Privacy and Identity Management for Life. Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes, and Ge Zhang, eds. Pp. 258–270. Berlin, Heidelberg: Springer Berlin Heidelberg. http://link.springer.com/10.1007/978-3-642-20769-3_21, accessed March 21, 2018.

Coiera, E. (2003).E-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment. Journal of the American Medical Informatics Association 11(2): 129–140.

Fatema, Kaniz, Ensar Hadziselimovic, H. J. Pandit, et al. (2017). Compliance through Informed Consent: Semantic Based Consent Permission and Data Management Model. *In* 5th Workshop on Society, Privacy and the Semantic Web–Policy and Technology (PrivOn2017), C. Brewster, M. Cheatham, M. d'Aquin, S. Decker and S. Kirrane, Eds, CEUR Workshop Proceedings, Aachen Pp. 1613–0073.

Friedman, Batya, Edward Felten, and Lynette I Millett (2000). Informed Consent Online: A Conceptual Model and Design Principles. University of Washington Computer Science & Engineering Technical Report 00–12–2: 8.

Hunton and Williams, (2016) A Guide for In-House Lawyers. https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2015/06/Hunton-Guide-to-the-EU-General-Data-Protection-Regulation.pdf.

Karjoth, Günter, Matthias Schunter, and Michael Waidner (2003). Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data. *In* Privacy Enhancing Technologies. Roger Dingledine and Paul Syverson, eds. Pp. 69–84. Berlin, Heidelberg: Springer Berlin Heidelberg. http://link.springer.com/10.1007/3-540-36467-6_6, accessed March 21, 2018.

Millett, Lynette I., Batya Friedman, and Edward Felten (2001). Cookies and Web Browser Design: Toward Realizing Informed Consent Online. *In* Pp. 46–52. ACM Press. http://portal.acm.org/citation.cfm?doid=365024.365034, accessed March 21, 2018.

Mont, Marco Casassa, Siani Pearson, Gina Kounga, Yun Shen, and Pete Bramhall, (2009). On the Management of Consent and Revocation in Enterprises: Setting the Context. HP Laboratories, Technical Report HPL-2009-49: 11.

Regulation (EU) 2016/ 679 (2016). Official Journal of the European Union L 119/1: 88.

Rissanen, Teemu (2016). Public Online Services at the Age of MyData: A New Approach to Personal Data Management in Finland: 12.

Rowan, W., Y. O'Connor, L. Lynch, and C. Heavin (2017.) Exploring User Behaviours When Providing Electronic Consent on Health Social Networks: A 'Just Tick Agree' Approach. Procedia Computer Science 121: 968–975.

Russello, Giovanni, Changyu Dong, and Naranker Dulay (2008). Consent-Based Workflows for

Healthcare Management. *In* Pp. 153–161. IEEE. http://ieeexplore.ieee.org/document/4556594/, accessed March 23, 2018.

Thuraisingham, Bhavani (2005). Privacy Constraint Processing in a Privacy-Enhanced Database Management System. Data & Knowledge Engineering 55(2): 159–188.

Vayena, Effy, and Alessandro Blasimme (2017). Biomedical Big Data: New Models of Control Over Access, Use and Governance. Journal of Bioethical Inquiry 14(4): 501–513.