Jurnal HAM
Volume 14 Nomor 2, Agustus 2023
DOI: http://dx.doi.org/10.30641/ham.2023.14.105-122

The Dynamic Consent for Optimizing Personal Data Protection and The Right to Privacy

(Persetujuan Dinamis sebagai Sarana Optimalisasi Pelindungan Data Pribadi dan Hak atas Privasi)

Masitoh Indriani[1]✉, Annida Aqiila Putri[2]
[1]Department of International Law, Faculty of Law, Universitas Airlangga
[2]Utrecht Law School, The Netherlands
✉masitoh@fh.unair.ac.id

ABSTRACT: Consent is one of the foundations for data processing in the Operation of Electronic Systems by government and private institutions. Implementing consent as a basis for data processing has several shortcomings, particularly as it primarily relies on individuals being aware of providing authentic consent. In practice, individuals often give consent without considering any terms and conditions. Consent obtained without knowledge of data processing can jeopardize the right to privacy and the protection of personal data. This paper examines dynamic consent as a means to optimize the protection of privacy rights. The findings indicate that the concept of dynamic consent that prioritizes its approach to Data Subjects serves as a means to optimize personal data protection. Dynamic consent can strike a balance between, on the one hand, the simplicity of the consent mechanism, and, on the other hand, the personal data protection standards and the right to privacy. Formulating dynamic consent should be based on legal elements, societal practices, technological features, and the involvement of personal data protection authorities. Additionally, as a form of implementing accountability for Electronic System Organizers as data controllers or processors, an effective mechanism for resolving personal data disputes is needed. These elements, when combined, can provide optimal personal data protection.

ABSTRAK: *Persetujuan (consent) merupakan salah satu dasar pemrosesan data dalam Penyelenggaraan Sistem Elektronik oleh institusi pemerintah dan sektor swasta. Implementasi pemberian persetujuan sebagai dasar pemrosesan data memiliki berbagai kekurangan, terutama pada tingginya ketergantungan terhadap kesadaran individu dalam mewujudkan persetujuan yang sah. Dalam praktiknya, individu kerap memberikan persetujuan tanpa memedulikan syarat dan ketentuan di dalamnya. Persetujuan yang diberikan tanpa pengetahuan akan informasi tentang pemrosesan data dapat mengancam hak atas privasi dan pelindungan data pribadi seseorang. Tulisan ini melakukan analisis tentang persetujuan dinamis sebagai sarana untuk mengoptimalkan pelindungan hak atas privasi. Hasil yang diperoleh memperlihatkan bahwa konsep persetujuan dinamis yang mengutamakan pendekatan terhadap Subjek Data hadir sebagai sarana optimalisasi pelindungan data pribadi. Persetujuan dinamis dapat menyeimbangkan antara kemudahan mekanisme persetujuan dengan tetap menjunjung tinggi standar pelindungan data pribadi dan hak atas privasi. Formulasi persetujuan dinamis didasarkan pada unsur hukum, praktik masyarakat, fitur teknologi serta keterlibatan otoritas pelindungan data pribadi. Selain itu, dibutuhkan mekanisme penyelesaian sengketa data pribadi yang efektif sebagai bentuk implementasi akuntabilitas bagi Penyelenggara Sistem Elektronik sebagai Pengendali atau Prosesor Data Pribadi. Gabungan dari elemen-elemen tersebut dapat menghasilkan pelindungan data pribadi yang optimal.*

Keywords:
consent;
dynamic consent;
personal data protection;
right to privacy

Kata Kunci:
persetujuan;
persetujuan dinamis;
pelindungan data pribadi;
hak atas privasi

Submitted/Diserahkan:
01-03-2023
Accepted/Diterima:
04-08-2023

How to cite/Cara Mengutip:
Indriani, Masitoh, and Annida Aqiila Putri. "Persetujuan Dinamis sebagai Sarana Optimalisasi Pelindungan Data Pribadi dan Hak atas Privasi". *Jurnal HAM*. Vol. 14 No. 2, Agustus 2023, 105-122). DOI. 10.30641/ham.2023.14.105-122)

1. Introduction

Technology plays an important role in various public service sectors in Indonesia, both involving government and digital commercial media. Digital-based government services such as e-KTP, electronic government (*e-government*),[1] and smart cities have developed in recent years.[2] Digital commercial media is also mushrooming, electronic commerce companies (e-commerce), electronic payment services (e-payment) to online transportation services are increasingly being used to encourage efficiency in people's lives.[3] To carry out the functions offered by digital services by the state as well as electronic commerce and financial technology media, it is necessary to process personal data. Therefore, the community as users must provide their personal data for processing in order to be able to access digital services to the fullest. One of the initial processes and mechanisms for processing personal data is through giving consent to digital-based service providers.

Various problems arise with the existence of a system that involves the processing of personal data. According to a report by Shurfshark, a company that focuses on cybersecurity, Indonesia is in the top three countries with the most data leaks globally in the third quarter of 2022.[4] In Indonesia, in 2022 there will be at least ten cases of leaks with a very large number.[5] Furthermore, according to a report written by CNN Indonesia, the majority of violations against personal data in the form of data leaks originate from applications belonging to the government or state institutions.[6] In the same year, the Ministry of Communication and Information of the Republic of Indonesia (hereinafter abbreviated as Kominfo RI) received 33 reports of incidents of violations of personal data.[7] These cases illustrate massive violations of personal data which correlate with increasingly massive intrusions on the right to privacy protected by the statutory regulations.

The presence of regulations regarding the protection of personal data is an important factor in tackling violations of personal data rights. Currently, the Government of Indonesia has a mechanism for protecting personal data which includes but is not limited to Law Number 11 of 2008 concerning Information and Electronic Transactions in conjunction with Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (hereinafter abbreviated as ITE Law). Article 26 of the ITE Law requires the processing of personal data through consent. In its development, the Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) in Article 20 also regulates consent as one of the bases for processing personal data. However, the imbalance of relations between the subjects involved in the processing of personal data cannot make consent legitimize the process of processing personal data. The imbalance in the relationship between the government, digital commercial media as private parties, and citizens as users is the biggest cause of the weakness of the consent mechanism in the processing of personal data. This imbalance occurs in relation to data processing agreements between users, electronic government administration, and private parties. Many users are not fully aware of the implications of data processing or do not clearly understand how users will use the data they have. In addition, users may not be fully informed about their rights or the options available to users regarding ownership of their data.

On the other hand, systems in e-government or the private sector may not provide sufficient information or transparency about data processing practices or may not prioritize protecting user privacy rights. It is this gap in understanding and communication that can lead to a lack of trust between users and the government sector which can hinder the effective and responsible use of data. For this reason, governments need to fill this gap by requiring that Personal Data Controllers and Personal Data Processors provide clear and easily accessible information about data processing practices, transparency about how data is collected and used, and ensure that users have meaningful options and control over their personal data.

1 Verdico Arief, "E-Government Di Asia Tenggara: Perbandingan Pengembangan E-Government Di Singapura, Malaysia Dan Indonesia," *Social Issues Quarterly* 1, no. 2 (2023): 345–62.
2 Digital Government, "E-Government Survey 2022" (New York, 2022).
3 Badan Pusat Statistik Republik Indonesia, "Statistik E-Commerce 2022" (Jakarta, 2022).
4 Surfshark Lab, "Data Breaches Rise Globally in Q3 of 2022," Data breaches rise globally in Q3 of 2022, accessed March 16, 2023, https://surfshark.com/blog/data-breach-statistics-2022-q3.
5 CNN Indonesia, "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah," accessed March 16, 2023, https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah.
6 Indonesia.
7 Tirah Arum Toewoeh, "Kominfo Gerak Cepat Tangani Lima Kasus Baru Kebocoran Data," Kementerian Komunikasi dan Informatika RI, accessed March 16, 2023, https://aptika.kominfo.go.id/2022/11/kominfo-gerak-cepat-tangani-lima-kasus-baru-kebocoran-data.

In connection with the regulation regarding the existence of legal obligations for Personal Data Controllers and Personal Data Processors and the granting of consent to the use of personal data, the General Data Protection Regulation (GDPR) is a reference and good practice regarding the regulation of legal obligations on the use of personal data, including how the basis for processing personal data is based on consent. The GDPR further categorizes an agreement and provides conditions for consent to be deemed legally valid. The consent must be voluntary (freely given), which means that the Data Subject does not need to sacrifice his rights if he refuses to give consent to the data processing.[8] In Indonesia, the consent used as the basis for the data processing is not voluntary consent. Considering that digital-based government services depend on the running of services through the processing of personal data in carrying out their functions, there is a potential for citizens to be unable to enjoy their rights if they refuse to give consent. This contrasts with the spirit of Open Government (OG) launched by the Government of Indonesia since 2012 which brings the spirit of ease of service to citizens.

The same condition also occurs in services run by the private sector. In the processing of data on commercial media, there are Terms and Conditions (S&C) and Privacy Policy as descriptions aimed at users which contain information about the use of their personal data. However, when examined further, the T&C and Privacy Policy of digital commercial media is a standard contract whose clauses have been determined regardless of the consumer's condition as a Data Subject. In the context of processing personal data, the standard contract does not provide freedom for Data Subjects to choose the extent to which data processing is carried out, and mechanisms for opting out are also not possible. As a result, when there is a breach of data or personal rights from the use of digital commercial media, the Data Subject is in a very vulnerable position.

In comparison, countries in the Regions of the European Union and Singapore[9] introduced dynamic consent as a form of protecting a citizen's personal data. Dynamic consent can be arranged in such a way as to accommodate different types of data subject needs according to the service context that places the data subject in a vulnerable position. The vulnerability of the Data Subject's position can also result in violations of fundamental rights, such as not being able to access bureaucratic services and other community services which is a citizen's rights. Not to mention there is the potential for violation of their privacy.

Currently, studies on the protection of the right to privacy and protection of personal data place a lot of emphasis on aspects of the form of crime[10] and the media or place where the violation occurs.[11] Furthermore, a study conducted by Rahman and Wicaksono states that personal data protection must be seen as part of the implementation of respect for Human Rights (HAM).[12] In line with that, the issue of consent which is one of the bases for processing personal data has not been widely discussed. In fact, consent as one of the entry points for data processing is currently considered to be insufficiently effective in protecting Data Subjects and more broadly must be seen as respecting their fundamental rights.[13] On the other hand, the excessive number of requests for consent in various electronic media can be a tiring experience and disrupt the user experience. Under these conditions, many users choose not to pay close attention to the conditions for giving the consent in question.

Furthermore, various problems also arise related to giving consent on digital platforms, including the issue of using personal data which has implications for a person's privacy, to issues of data security. Problems arise due to the lack of clarity in the Privacy Policy offered by the platform. The information contained in these policies is often presented in legal language that some people find difficult to understand. As a result, users give their consent under conditions of not really understanding the content, especially in relation to how their personal data will be used. Another problem is the use of the default opt-in consent mechanism. This standard consent strategy leaves no choice for the user. The result is that users will not knowingly know that they are giving permission to have their personal data processed. The next problem is that users are faced with a system that does not provide the convenience to withdraw their consent, resulting in no full control over the use of their personal data.

---

8 The European Commission, "Opinion 15/2011 on the Definition of Consent," Opinion 15/2011 on the definition of consent, accessed March 16, 2023, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

9 Advisory Guidelines et al., "Advisory Guidelines on Requiring Consent for Marketing Purposes" (Singapore, 2015).

10 Indriana Firdaus, "Upaya Pelindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan," *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 23–31, https://doi.org/10.52005/rechten.v4i2.98.

11 Umi Sugiyanti and Agung Pambudi, "Pelindungan Data Privasi Dan Kebebasan Informasi dalam Platform WhatsApp," Jurnal IPI (Ikatan Pustakawan Indonesia 7, no. 2 (2022): 60–70.

12 Faiz Rahman and Dian Agung Wicaksono, "Researching References on Interpretation of Personal Data in the Indonesian Constitution," Jurnal Penelitian Hukum De Jure 21, no. 2 (2021): 187, https://doi.org/10.30641/dejure.2021.v21.187-200.

13 Bart W. Schermer, Bart Custers, and Simone Van der Hof, "The Crisis of Consent," Ethics and Information Technology, no. 2007 (2014): 1–19, https://doi.org/10.1007/s10676-014-9343-8.

Thus, we need to underline the importance of developing the concept of dynamic consent as an entry point for data processing in services provided by the electronic-based government as well as goods and services by the private sector to provide protection for citizens' fundamental rights. In general, this concept of dynamic consent provides an opportunity for users or citizens to retain full control over the use of their personal data because the digital-based service provider provides a mechanism for granting approval based on full dynamic control. Thus, there is a real mechanism for Data Controllers from both public institutions and digital service providers managed by the private sector. The development of this mechanism is carried out by implementing data processing based on dynamic consent so that digital platforms will be able to strengthen the right to user privacy and be able to manage risks in the event of a violation of the use of personal data to comply with the statutory regulations.

Based on the background description, this paper examines two things. First, the urgency of developing dynamic consent as a basis for processing personal data and; Second, the formulation of dynamic consent as a form of personal data protection in digital services by Public Electronic System Operators (PSE) and services by private PSE. This article is organized into six sections; The first and second sections discuss the development of the use of digital-based public services by public Electronic System Operators and the utilization of products and services by private Electronic System Operators which in their mechanism use personal information; The third and fourth sections discuss the principles of personal data protection in electronic systems and the position of consent in the processing of personal data in electronic systems; The fifth and sixth sections discuss the development of dynamic consent in several countries and efforts to develop dynamic consent formulations as a means to optimize privacy protection in electronic media (platforms).

2. Method

The method used in this study is a qualitative research method, using secondary data in the form of literature studies (document reviews). The secondary data collected is reading material/legal materials consisting of reading material related to the concept of consent in processing personal data as well as the concept of informed consent in the medical world which is used as an initial reference in the development of dynamic consent. Apart from that, we also refer to other legal documents including the ITE Law, the PDP Law, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Transaction Systems, and Minister of Communication Regulation Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems as well as documents and texts academic regulations and relevant government reports relating to the concept of consent and processing of personal data.

The collected data were analyzed and presented descriptively. In conducting the analysis, the authors rely on the concept of dynamic consent in informed consent used in medical practice in order to be able to identify elements regarding consent that have not been regulated by norms in Article 26 of the ITE Law and Article 20 paragraph (2) letter a of the PDP Law in conjunction with Article 21 of the PDP Law. Then, this study obtains elements that can support the development of the concept of dynamic consent with an approach to Data Subjects that have been regulated normatively in these statutory regulations.

3. Discussion

3.1 Development of Digital-Based Public Services and Their Legal Framework

In principle, electronic government is the use of information technology by the government in providing information and services to its citizens, including business affairs, as well as other matters relating to government. Electronic government can be applied to legislative, judicial, or public administration which aims to increase the internal efficiency of the government organization itself, deliver public services, or processes of democratic governance. The digital-based public service model can take the form of Government-to-Citizen or Government-to-Customer (G2C), Government-to-Business (G2B), and Government-to-Government (G2G). The most expected advantages of electronic government are increased efficiency, convenience, and better accessibility of public services.[14]

14 Firdaus Masyhur, "Penelitian E-Government Di Indonesia: Studi Literatur Sistematis Dari Perspektif Dimensi Pemeringkatan e-Government Indonesia (PeGI)," *JURNAL IPTEKKOM : Jurnal Ilmu Pengetahuan & Teknologi Informasi* 19, no. 1 (2017): 51, https://doi.org/10.33164/iptekkom.19.1.2017.51-62.

Services that have been used so far are familiar, for example, an activity planning system (e-planning), a budget execution system (e-budgeting), a goods and/or service procurement system (e-procurement), and many more. These various digital-based public services are a sign that government administration is quite responsive in keeping abreast of technological and information developments. Various government services based on electronic systems in electronic government are expected to provide services effectively and efficiently. Service innovation in the form of electronic government is also the key to service transformation.

In its development, the smart city concept has become a separate phenomenon as a concept that offers integrated technology-based public services as developed in the 100 smart city movement program initiated by the Ministry of Communication and Informatics, Ministry of Home Affairs, Ministry of Public Works and Public Housing (PUPR), the National Planning Agency (Bappenas) and the Presidential Staff Office (KSP). The 100 smart city movement aims to provide guidance to Regencies/Cities in compiling a Smart City Masterplan so that they can maximize the use of technology, both in improving community services and accelerating the potential that exists in each region.[15]

In fact, the implementation of electronic government based on the smart city program is still dealing with old problems, namely problems related to bureaucracy. In addition, the practice and implementation of smart cities that rely on cooperation with third parties in the management and development of their systems also raise several potential problems considering a large amount of various data, including personal data managed by third parties.[16]

In its development, based on the 2022 United Nations e-government Survey report, the e-Government Development Index (EDGI) or electronic government ranking, Indonesia is ranked 77th globally; up eleven ranks compared to the survey conducted in 2020.[17] In the ASEAN region, Indonesia ranks fifth with a score of 0.7160 points out of 1. Singapore ranks first with a score of 0.9133 points out of 1 and makes it the rank twelfth globally.[18] The basis for a survey conducted by the United Nations, in particular by the UN Department of Economic and Social Affairs, is to see how e-government can facilitate integrated policies and services in the dimension of sustainable development. This survey is the only global survey that assesses the development status of the electronic government of 193 UN member states. This survey also serves as a tool for countries to learn to identify strengths and challenges in implementing electronic government, as well as formulating policies and strategies in the field of public services. In addition, this survey aims to facilitate discussions between UN organs, including the UN General Assembly and the UN Department of Economic and Social Affairs, on issues related to electronic government.[19]

The implementation of this electronic government program or e-government actually has another dimension that is felt by users of public services. In this case, there is a demand for the government to significantly improve its performance based on information and communication technology.[20] By transforming through these electronic government-based services, the government is expected to be able to optimize its services to reduce bureaucratic problems. One way is to form a management system network that has integrated work processes with the aim of simplifying access to all public service information. Thus, there is a guarantee that information and communication technology-based public services can run optimally.

In 2018, Presidential Regulation Number 95 of 2018 was issued concerning Electronic-Based Government Systems (hereinafter abbreviated as Perpres SPBE). This Perpres SPBE emerged based on various problems regarding governance that were not integrated and unified, resulting in a waste of budget due to duplication of service applications and infrastructure. The policies in this Perpres SPBE focus on three things, namely: First, integration of government business processes; Second, implementation of data and service integration; and Third,

15 Leski Rizkinaswara, "Gerakan Menuju 100 Smart City," accessed March 16, 2023, https://aptika.kominfo.go.id/2022/07/gerakan-menuju-100-smart-city-2/.

16 Masitoh Indriani and Ekawestri Prajwalita Widiati, "The Privacy Challenge in the 'Smart Era': A Study of the Implementation of e-Government in Surabaya," ICPS 2018 Proceeding, no. Icps (2019): 641–44, https://doi.org/10.5220/0007548606410644.

17 Saefudin, "Signifikan, Hasil Survei e-Government Indonesia Naik 11 Peringkat," accessed March 16, 2023, https://aptika.kominfo.go.id/2022/10/signifikan-hasil-survei-e-government-indonesia-naik-11-peringkat/.

18 Saefudin., accessed March 16, 2023.

19 the United Nations, "The United Nation E-Government Survey 2022: The Future of Digital Government" (New York, n.d.), https://desapublications.un.org/sites/default/files/publications/2022-09/Web version E-Government 2022.pdf.

20 Vani Wirawan, "Penerapan E-Government Dalam Menyongsong Era Revolusi Industri 4.0 Kontemporer Di Indonesia," Jurnal Penegakan Hukum Dan Keadilan 1, no. 1 (2020): 1–16, https://doi.org/10.18196/jphk.1101.

the integration of ministries and government agencies. This policy is expected to improve: efficiency in the use of information technology, service integration through common applications, transparency and public participation, budget efficiency, bureaucratic reform, and data integration between ministries and government agencies.

Furthermore, in 2019, Presidential Regulation Number 39 of 2019 concerning One Data Indonesia (Perpres on One Data) was issued. Perpres on One Data is a government data governance policy to produce data that is accurate, up-to-date, integrated, and accountable, as well as easily accessible and shared between central agencies and regional agencies. Data produced by data producers must be based on the following principles: First, meet data standards; Second, it has metadata; Third, comply with the rules of data interoperability; and Fourth, use reference codes and/or master data. The concept promoted in One Data Indonesia gives hope for guaranteeing data integrity and as a form of fulfilling the need for quality data for the community. In addition, by adhering to the principle of open data, this policy will increase government transparency and accountability, as well as increase community participation in overseeing the development implementation process.

Moreover, the two legal frameworks above at least provide an analytical basis for Data Processors and Data Subjects to understand data management procedures (data governance). In the context of the Open Government (OG) movement, the implementation of electronic government will increasingly emphasize that the two main principles in implementing OG, namely participation and transparency, will always be the basis for the implementation of the services provided.

In terms of consent, all media have the same mechanism, namely data processing. The characteristics of giving consent to public services are one-way. Referring to Kurbalija, this one-way nature is illustrated in that the government collects various personal information of citizens in the form of population documents, social documents to the criminal records of its citizens.[21] Information or data collected by the government cannot be rejected by citizens. Instead, various government agencies continue to process the data. This collection of information and data poses a challenge in ensuring the balance of data processing as part of efforts to implement electronic government by guaranteeing the fundamental rights of citizens.[22]

3.2 Digital Business Ecosystem Growth

Developments in technology and information have also significantly influenced the business model of trade and the service sector in Indonesia. Various application-based services are growing very rapidly. Government policy through the 1000 Digital Startup Movement marks the creation and development of Indonesia's digital economy. The development of the digital industry also has a significant influence on increasing Indonesia's gross domestic product (GDP).[23]

In its development, the government formulated 5 (five) principles in the development of e-commerce as one of the main pillars of the digital business ecosystem. First, all Indonesian citizens have the same opportunity to access and become e-commerce actors. Second, all Indonesian citizens have knowledge and awareness so they can take advantage of information technology for the economy. Third, minimizing the loss of jobs during the transition era towards the digital economy. Fourth, the implementation of legal instruments and policies must support e-commerce security which includes technology neutrality. Fifth, local e-commerce businesses, especially startups and Small and Medium Enterprises (SMEs), must be given adequate priority and protection, with a focus on international transparency and consistency.

The main activity of e-commerce in Indonesia currently relies on good applications based on online marketplace platforms. According to a survey conducted by Kadence International, users are very concerned about security and service quality.[24] These two things are also notes related to the level of user satisfaction. The security and quality of service in question are related to product quality, delivery, and payment security. Apart from e-commerce, the development of online-based financial services or financial technology (fintech) is also very rapid. Services supporting e-commerce activities that have been registered with the Financial Services Authority (OJK) of the Republic of Indonesia are considered to have a high level of security and are well

21 Jovan Kurbalija, *An Introduction to Internet Governance*, Diplo Foundation (Diplo Foundation, 2014).
22 Kurbalija.
23 Rizkinaswara, "Gerakan Menuju 100 Smart City."
24 Isna Rifka Sri Rahayu, "Hasil Survei: Promosi Tak Lagi Jadi Penentu Utama Pilih e-Commerce," accessed March 16, 2023, https://money.kompas.com/read/2022/12/08/171000026/hasil-survei--promosi-tak-lagi-jadi-penentu-utama-konsumen-pilih-e-commerce?page=all.

encrypted. This is shown by the results of a survey conducted by the OJK through the 2022 National Financial Literacy and Inclusion Survey (SNLIK) which stated that the literacy and inclusion index increased compared to 2019.[25] Literacy and inclusion are considered capable of providing a significant and strategic role in accelerating economic recovery by still referring to consumer protection.

In its development, the use of electronic systems with e-government and e-commerce is a form of technological progress that can encourage efficiency and convenience. However, its use can also threaten people's right to privacy. Electronic Systems depend on the utilization of personal information provided by users. These digital-based services can be enjoyed or accessed by providing personal information in an electronic system. One application can store more than hundreds of thousands of users' personal data, in line with the number of users of that application. The use of these applications actually imposes certain burdens in the form of rights and obligations for consumers (users) and Electronic System Providers (PSE) within an electronic transaction scope. These rights and obligations can be seen the first time a user wants to use an application which is usually represented in a Terms of Service (ToS) and Privacy Policy. A user must provide some of their personal information to be able to take advantage of the services of PSE. Conversely, if users do not provide their personal information, then they will not be able to use these applications. This condition is unbalanced and can lead to potential legal problems in its implementation.

One of the negative impacts of the utilization of this personal information is if PSE is unable to maintain the confidentiality of a user's personal information properly. A study conducted by Stony Brook University and the University of Massachusetts found that more than 70% of smartphone applications share personal data with third parties.[26] Not to mention the many cases of misuse of personal information which, when traced, are closely related to the processing of such personal information. The cases that occurred also illustrate that PSE is unable to provide adequate protection for a user. In other words, consent in providing personal information is the starting point for citizens to be able to take advantage of these digital services. In its implementation, the formulation of consent given to enjoy access and service has the potential to become a measuring tool related to the level of legal compliance of Data Controllers and Data Processors.

3.3 Principles of Personal Data Protection in Electronic Systems

Data processing in PSE can be in the form of collection, storage, use, change, deletion, and various other forms that are carried out as part of using PSE services. For this reason, guidance for PSE in terms of processing personal data is necessary. Currently, there are several legal instruments to protect personal data as well as to protect the right to privacy. In the European Union, prior to the enactment of the General Data Protection Regulation (GDPR) in 2016, there was The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981 or better known as the Council of Europe Convention 108 (known as Convention 108). This convention is an international instrument the first legally binding in the field of data protection and privacy. In its development, there is Directive 95/46/EC which contains a framework for protecting individuals regarding the processing of personal data and the freedom of movement of this data. Outside the European Union, the Organization for Economic Co-operation and Development (OECD) also issued the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980 and has now been updated in 2013. These guidelines have two main objectives, namely: to provide privacy standards and to facilitate the free flow of information for law enforcement activities. From these international instruments, in general, the same general principles can be drawn regarding the protection of personal data. The principles of personal protection in general also apply to each personal data processing cycle.

Six personal data protection principles apply to each type of processing. The first principle is legitimacy, fairness, and transparency. PSE is prohibited from carrying out any kind of unlawful data processing. In addition, PSE also has an obligation to disclose the purpose, intent, and form of processing personal data to the Data Subject. Second, limiting the purpose, namely, the collection of personal data is limited by data that is relevant for the smooth functioning of the services carried out by PSE. The use of personal data by PSE can only be

25 Abdul Malik, "Survei OJK 2022 : Inklusi Keuangan Naik Jadi 85,1% Dan Literasi 49,6%," accessed March 16, 2023, https://www.bareksa.com/berita/pasar-modal/2022-10-30/survei-ojk-2022-inklusi-keuangan-naik-jadi-851-dan-literasi-496.

26 Abbas Razaghpanah et al., "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem," in *Proceedings 2018 Network and Distributed System Security Symposium* (Reston, VA: Internet Society, 2018), https://doi.org/10.14722/ndss.2018.23353.

carried out after obtaining consent from the Data Subject, and may not be used for purposes other than what has been approved. Third, data minimization, namely personal data must be obtained legally, not excessively, and in accordance with the intended use of the personal data in PSE. Fourth, data accuracy, namely changes to personal data refers to the principle of personal data accuracy. PSE has an obligation to take steps to ensure that the data it has is accurate, complete, relevant, not misleading, and is the latest data. Fifth, data storage limitations, in this case, data storage is limited by the period required for its intended use.[27] PSE has the obligation to delete personal data that is no longer relevant, inaccurate, or based on a request from the Data Subject. This refers to the principle that the processing of personal data must be carried out on a specific basis, purpose, or agreement.[28] Without this basis, personal data must be deleted. Sixth, integrity and confidentiality. This principle refers to the technical steps that must be taken by PSE in ensuring the security of personal data from threats of damage, theft, and unlawful processing of data that can harm the Data Subject.[29]

These protection principles are very important to note as the main foundation in protecting the right to privacy. This is based on the fact that the processing of personal data in e-government and e-commerce electronic systems is closely related to the right to privacy. The right to privacy at the beginning of its development can be interpreted as the right to be left alone.[30] The right to privacy is also broadly defined as the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.[31] Privacy can be grouped into various aspects; the first aspect is physical, which involves the body physically and mentally, such as DNA, blood tests, and urine tests; the second aspect is territorial, which relates to a place and can indicate the location of a residence or house. This aspect of privacy is related to the right to security and communication, which includes correspondence and human relations. The right to privacy in this dimension is related to wiretapping activities and the secrecy of correspondence, as well as personal information relating to a person's data.

The right to privacy is recognized as a human right contained in Article 12 of the Universal Declaration of Human Rights (UDHR). This right protects privacy from arbitrary interference.[32] Furthermore, the right to privacy is also protected by Article 17 of the International Covenant of Civil Political Rights (ICCPR). Article 17 of the ICCPR not only gives the obligation to protect its citizens through regulations but also prohibits violations of privacy.[33] The privacy regulation in the ICCPR is the strongest legal basis in international law.[34] These international instruments provide an overview of the legal framework for a state in providing protection and promoting the right to privacy. Thus, a country is expected to adopt and implement the principles in these instruments into policies and actions in the country.

In Indonesia, the right to privacy is constitutionally contained in Article 28 G of the Constitution of 1945. The right to privacy in the Constitution of 1945 is interpreted through the phrase "... the right to feel safe and protected from threats of fear to do or not do something that is a human right." In addition, Indonesia is also a country that has ratified the ICCPR which passed through Law No. 12 of 2005. Therefore, Indonesia has obligations within the constitutional and international spheres related to respect for the right to privacy.[35]

The right to privacy is one of the bases for the formulation of the right to protection of personal data.[36] The protection of personal data is one of the efforts to fulfill the right to privacy. For that, both are elements

27 Sinta Dewi Rosadi, "Pelindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara," *Kebebasan Berekspresi Di Indonesia: Hukum, Dinamika, Masalah Dan Tantangannya*, 2016, 210.

28 Wahyudi Djafar, Miftah Fadli, and Lintang Setianti, *Desain Kebijakan Tata Kelola Konten Internet: Usulan Pelembagaan Dari Perspektif Hak Asasi Manusia*, 2017.

29 Rosadi, "Pelindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara."

30 Samuel D Warren and Louis D Brandeis, "The Right to Privacy," Harvard Law Review 4, no. 5 (1890): 193–220, https://doi.org/10.2307/1330091.

31 Alan F. Westin, Privacy and Freedom (New York: Atheneum Press, 1967).

32 Asbjorn Elde, Alfredsson Gudmundur, and Göran Melander, *The Universal Declaration of Human Rights: A Commentary* (Oslo: Scandinavian University Press, 1992).

33 Nihal Jayawickrama, *The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence* (Cambridge: Cambridge University Press, 2002).

34 Lee A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties," *International Journal of Law and Information Technology*, 1998, 4.

35 Rosadi, "Pelindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara."

36 Human Rights Committee General Comment, "On the Right To Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation," vol. I, 2013.

that cannot be separated. In data processing activities, individuals have the right to determine the conditions for implementing personal data processing.[37] This is a form of fulfilling the right to privacy as a fundamental right, as well as individual rights as Data Subjects. Thus it can be understood that the context of personal data protection is an embodiment of respect for the right to privacy.

3.4 Position of Consent in Personal Data Management

In an effort to protect personal data, the processing of personal data must be legally based. One of the legal bases for processing personal data that is often used by PSE is consent. In principle, consent is defined as a condition that occurs when a person voluntarily agrees to the wishes of another person. The term consent is a general term used followed by a specific definition used in certain fields such as law, medicine, research, sexual relations, and so on which represents a person's consent to another party outside himself.

In processing personal data, the consent of a Data Subject to a Data Controller establishes a legal relationship that results in rights and obligations for both parties. On the one hand, the Data Subject, by giving consent, has acknowledged the ownership of the personal data for himself and consciously implements his rights. On the other hand, the Data Controller is burdened with the obligation to strive for the highest protection of the Data Subject's personal data from threats that could interfere with the Data Subject's rights.

Judging from the history of regulation, the concept of consent as the legal basis for processing personal data has existed since the first domestic regulations on personal data appeared in Europe in 1970.[38] However, the concept of consent is not always taken literally. In France, the concept of consent contained in the regulation on the protection of personal data is not specifically explained but is interpreted in the jurisprudence of the Data Protection Authority (DPA). In England, the common law system develops the concept of agreement in more specific sectors, depending on the context in which the agreement is used.[39]

Along with the development of regulations regarding the protection of personal data in Europe, the definition of consent is also growing. Convention 108 is one of the legal instruments that stipulates consent as the legal basis for processing personal data with criteria including free, specific, well-informed, and unambiguous. The climax is through the ratification of the GDPR, which in Article 4 (11) stipulates four provisions regarding consent. First, consent is given voluntarily. Giving consent voluntarily means consent is given without coercion from the Data Controller. Data Controllers may demonstrate that the consent they obtained from the Data Subject was given voluntarily, including through granting access to electronic system services, regardless of whether such consent has actually been given or not. For example, in the use of cookies on websites, even if the Data Subject does not give consent to cookies, the Data Subject can still access the site. This illustrates that the consent given by the Data Subject is not an act of exchanging or bartering for electronic system services by giving consent to the processing of their personal data. Second, the specific Consent requested by the Data Controller must be in accordance with the purpose conveyed to the Data Subject. This requirement prohibits the existence of 'one consent for all' or the use of one consent for a purpose to be used as a basis for other data processing purposes. Third, information, where the Data Controller must provide correct and accurate information to the Data Subject regarding the purpose of data processing, how the data will be processed, who will process the data, and all details regarding data processing before the Data Subject gives their consent. This is intended so that the consent given by the Data Subject can be considered taken in a conscious condition of the processing of personal data that will be carried out. Fourth, a clear indication, namely that consent must be given by the Data Subject openly. The Data Controller may not simply assume that consent has been given without explicitly stating that consent has been given.[40]

These four elements are cumulative requirements for using consent as the basis for data processing.[41] With these provisions in place, the Data Controller is no longer only obliged to show consent but is also burdened to prove that the consent given by the Data Subject has fulfilled the specified conditions.

37 Rosadi, "Perlindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara."
38 Working Party 29, "Opinion 15/2011 on the Definition of Consent," 2011.
39 Working Party 29.
40 Working Party 29.
41 Working Party 29.

In Indonesia, the legal basis for consent as the basis for processing personal data is regulated in Article 26 of the ITE Law and Article 20 paragraph (2) letter a of the PDP Law. The consent in this Article 26 of the ITE must be given in writing by the owner of the personal data, either manually or electronically, after the owner has been given a full explanation of any action to be taken in relation to their personal data including cross-border transfers. These provisions are much simpler than the consent requirements governed by the GDPR. When compared, the consent requirements in Article 26 of the ITE Law only meet the third and fourth requirements of the GDPR, namely the approval must be based on information and is affirmative. Many of its implementations have been found in the form of signs of approval of the Terms and Conditions (T&C) and Privacy Policy in electronic systems. The Data Controller is not burdened by this provision. Meanwhile, Article 20 paragraph (2) letter a of the PDP Law explains that as one of the bases for processing personal data, granting this consent places a very large burden on the Data Controller to convey information related to the legality and purpose of processing, the type, and relevance of the data to be processed, the retention period for documents containing personal data, details regarding the information collected, the processing period and the rights of the Data Subject.

On the one hand, the concept of consent referred to in the GDPR, the ITE Law, and the PDP Law, is not a perfect basis for personal data protection. In the context of the European Union, Data Controllers must also ensure that they comply with all other requirements of the GDPR, including the principles of transparency, limitation of purpose, data minimization, accuracy, limitation of retention, and accountability. Consent is one of the legal bases for processing personal data. However, once again simply obtaining consent from the Data Subject is not sufficient to ensure GDPR compliance. Under Article 6 of the GDPR, there are specific requirements for obtaining valid consent, including that it must be given freely, specifically, informedly, and expressly. This implies that individuals must be fully informed of what they are consenting to and have the ability to withdraw their consent at any time.

In addition to obtaining valid consent, the Data Controller must also ensure that any processing of personal data is necessary and proportionate to the purposes for which they were collected. They should also ensure that appropriate technical and organizational measures are in place to ensure data security and protect the rights and freedoms of Data Subjects. Currently, the problems that often arise from the use of consent as the basis for personal data processing are the high dependence on individual awareness and the existence of an excessive burden of consent (consent overload) in society which is a condition that describes a situation where individuals are required to give their consent to processing their data in very large quantities and continuously, either directly or indirectly. This is especially the case in the context of digital services and the use of technology, where companies or in this case the private sector often seek approval for various purposes, including tracking user behavior and using data for marketing purposes (targeted advertising).[42]

The problem with consent overload is that individuals may not fully understand the implications of their consent or may even feel compelled to give consent because they do not want to lose access to the services they need.[43] Additionally, excessive consent requests can become tiresome and disrupt the user experience. One of the biggest criticisms of the consent mechanism is its reliance on each individual's personal conscience to provide them with care.[44] In practice, almost all internet users do not read the existing T&C and privacy policy.[45] Even though some have read it, it is not certain that the Data Subject understands the provisions contained therein and the consequences that may arise due to the processing of personal data that they agree to.[46] In fact, the Privacy Policy in question can be categorized as one of the legal documents in the implementation of personal data processing as well as one of the indicators that PSE complies with legal provisions on personal data protection.[47]

In addition, today's society is also faced with a situation where there is giving consent as well as receiving excessive information. This can cause the individual's choice to give their consent to lose its meaning (absence

42 Benedikt Buchner and Merle Freye, "Informed Consent in German Medical Law: Finding the Right Path between Patient Autonomy and Information Overload," in SSRN Electronic Journal, 2022, https://doi.org/10.2139/ssrn.4088631.
43 Role in Protecting Patients and Preventing Overwhelm," AMA Journal of Ethics 18, no. 9 (2016): 869–86, https://doi.org/10.1001/journalofethics.2016.18.9.peer2-1609.
44 Schermer, Custers, and Van der Hof, "The Crisis of Consent."
45 Internet Society, "Global Internet Survey, Summary Report," n.d.
46 S. Brockdorff, N.; Appleby-Arnold, "What Consumers Think," *EU Consent Project*, 2015.
47 John Lister, "Privacy Policies Are Legally Required," accessed March 16, 2023, https://www.freeprivacypolicy.com/blog/privacy-policy-legally-required/.

of meaning).[48] As a result, individuals give their consent easily regardless of the consequences and threats to their right to privacy. This drastically reduces the effectiveness of the consent mechanism on which personal data is processed. The consent given including those that have fulfilled the requirements is meaningless. Rights and obligations that arise with consent cannot be applied.

On the other hand, consent is the most easily implemented basis for processing personal data for controllers and Data Subjects. Other fundamentals of personal data processing under the GDPR such as the existence of a legitimate interest, contractual necessity, or vital interest and legal processing of personal data are difficult to implement in countries that do not yet have complete personal data protection regulations. These grounds require obligations to be detailed in the law.[49] Measuring compliance (legal compliance) will be more difficult to do on personal data processing mechanisms on these grounds without comprehensive personal data protection regulations. Thus giving consent is the answer to this situation.

Individual autonomy over their own privacy rights which is made possible by a consent mechanism can be a form of responsibility to Data Controllers that has not been regulated by law. In the aspect of the relationship between Data Subjects as consumers, there are economic demands for PSE to maintain the trust of users of their electronic system services.[50] Consumers as Data Subjects will choose electronic system services that have the safest protection of personal data to avoid things that can harm them. This can be seen in the case of Facebook, which experienced a decrease in user activity after the disclosure of the case of buying and selling personal data with Cambridge Analytica.[51] Therefore, the obligations of the Data Controller in countries where there are no detailed regulations regarding the protection of personal data can still be enforced by consent.

3.5 Development of Dynamic Consent

The development of forms of electronic system administration encourages the formation of a dynamic personal data protection mechanism without compromising the right to privacy and security of Data Subjects. This is inseparable from the condition of the community which is faced with a high burden to give consent (consent overload). Some of the causes for this burden are related to technical issues of implementing flexibility in the field[52], regulatory complexity, user awareness, and understanding[53], absence of industry standards and guidelines[54], and resistance from organizations responsible for processing personal data[55].

Dynamic consent is a solution to reduce imperfect consent as a basis for processing personal data so that the protection provided remains maximum while providing high flexibility for Data Controllers and Data Subjects. Dynamic consent is the term used to describe online personalized consent on communication platforms.[56] Conceptually, dynamic consent is different from specific consent.[57] Dynamic consent can be set up to accommodate different types of Data Subject needs according to context.[58] Even so, both are forms of the opposite of consent that includes all data processing (blanket consent).[59]

Dynamic consent provides more flexibility in implementing agreements as a form of individual autonomy. Dynamic consent respects the preferences of Data Subjects in the processing of their personal data. These

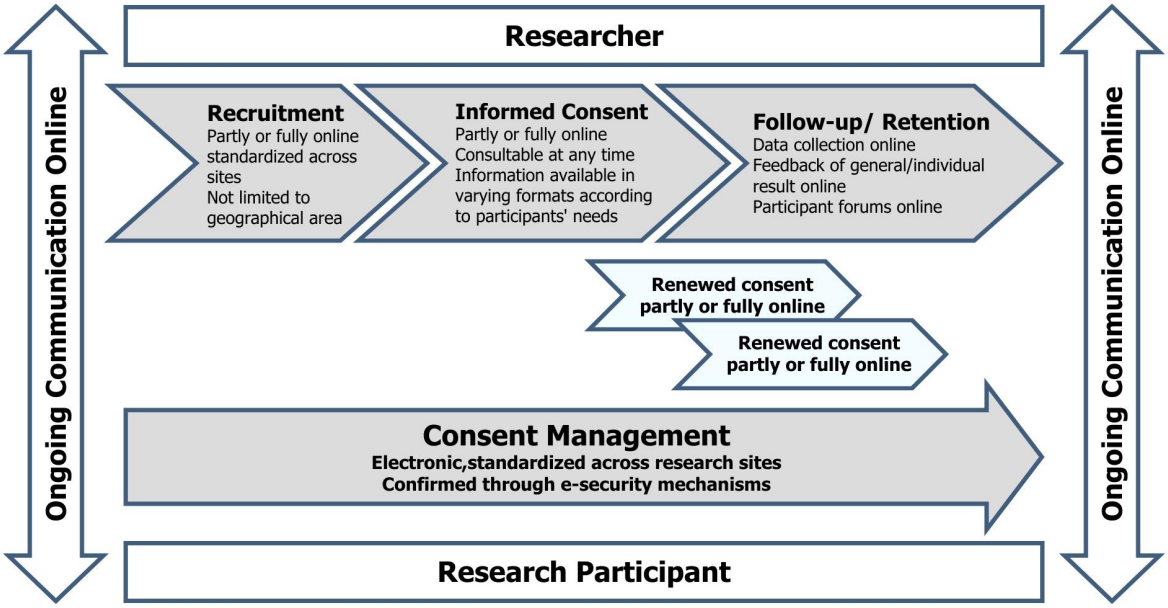
48 Schermer, Custers, and Van der Hof, "The Crisis of Consent."
49 Edward S. Dove and Jiahong Chen, "Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis," *International Data Privacy Law*, 2020.
50 UK Information Commissioner's Office, "Guide to the General Data Protection Regulation," 2019.
51 Alex Hern, "Facebook Usage Falling after Privacy Scandals, Data Suggests," *The Guardian, June* 2019.
52 Harriet J.A. Teare, Megan Prictor, and Jane Kaye, "Reflections on Dynamic Consent in Biomedical Research: The Story so Far," European Journal of Human Genetics 29, no. 4 (2021): 649–56, https://doi.org/10.1038/s41431-020-00771-z.
53 Buchner and Freye, "Informed Consent in German Medical Law: Finding the Right Path between Patient Autonomy and Information Overload."
54 Eva Schlehahn, Patrick Murmann, and Farzaneh Karegar, "Opportunities and Challenges of Dynamic Consent in Commercial Big Data Analytics," in IFIP International Summer School on Privacy and Identity Management (Springer, 2020), 29–44, https://doi.org/https://doi.org/10.1007/978-3-030-42504-3_3.
55 Buchner and Freye, "Informed Consent in German Medical Law: Finding the Right Path between Patient Autonomy and Information Overload."
56 Jane Kaye et al., "Dynamic Consents: A Patient Interface for Twenty-First Century Research Networks," *European Journal of Human Genetics* 23 (2015): 3.
57 Isabelle Budin-Ljøsne et al., "Dynamic Consents: A Potential Solution to Some of the Challenges of Modern Biomedical Research," BMC Medical Ethics 18, no. 1 (2017): 1–10, https://doi.org/10.1186/s12910-016-0162-9.
58 Harriet J.A. Teare, Megan Prictor, and Jane Kaye, "Reflections on Dynamic Consents in Biomedical Research: The Story so Far," European Journal of Human Genetics 29, no. 4 (2021): 649–56, https://doi.org/10.1038/s41431-020-00771-z.
59 UK Information Commissioner's Office, "Guide to the General Data Protection Regulation."

preferences can be reviewed from time to time and changed according to changes in the preferences of the Data Subject. In order to ensure that Data Subjects know their preferences, dynamic consent is complemented by the accessibility of information about data processing accompanied by interaction and participation between Data Subjects and Data Controllers. In other words, the dynamic consent system can answer doubts about the dependence on individual autonomy in the form of ordinary consent.

Dynamic consent refers to an approach that engages individuals regarding the use of their personal information that grants rights to owners of personal data (Data Subjects) and collectors of personal information. This dynamic consent then leverages interactive interface-based technologies that support competent individuals in making autonomous decisions to change their consent choices in real-time.[60] Through these online media, such Data Subjects may, for example, agree or refuse the collection of their personal information or record preferences for data sharing with third parties.

Historically, this dynamic consent method has limited use in the medical and scientific research fields. This is supported by the nature of these two fields which are developing rapidly in accordance with new discoveries from the research conducted, so that there are frequent changes in the purpose of processing respondent data.[61] Traditional consent systems are difficult for researchers because researchers often have to manually seek re-consent when developments occur in their research. Whereas through dynamic consent, the researchers already know the data subject's preferences from the start which then establish limits on the extent to which the researchers can process the data. That way, the processing of personal data can still be carried out safely and legally, but still dynamic and adaptive.

Figure 1. Scheme of Dynamic Consent in Scientific Research

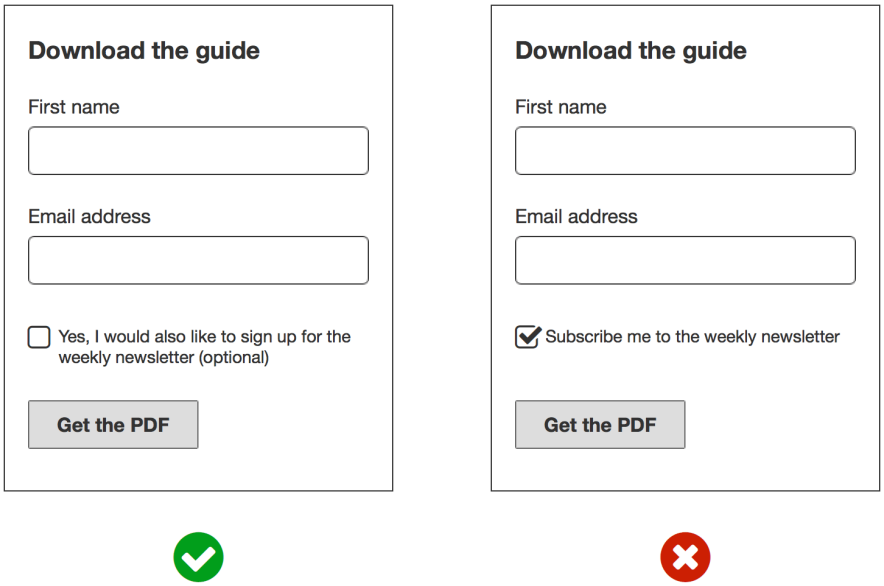


Source: Budin-Ljøsne, et.al, 2017

In Figure 1, a researcher as a Data Processor is actively involved from the start of data collection in the participant recruitment process. With ongoing online communication, researchers guide participants in giving initial consent until the time when the consent needs to be renewed. This shows the participation of both parties, namely the Data Subject and the Data Controller while still emphasizing the existence of control from the Data Subject over the data being processed

60 Kaye et al., "Dynamic Consents s: A Patient Interface for Twenty-First Century Research Networks."
61 Kaye et al.

Figure 2. General Form of Consent in the Implementation of Electronic Systems (Left Side GDPR Eligible)



Source: Iubenda, 2019

Figure 2. shows that the menu on the left of the image is a form of giving consent that meets GDPR requirements, namely by having a box that has not been filled in beforehand (checked/pre-ticked) and in general using a clear and specific language. Meanwhile, the right side shows an element of coercion by providing language that is less straightforward as a condition for downloading the document to be requested. Thus, it is necessary to emphasize that the participation of a user is key in the implementation of dynamic consent. This participation can be seen from the beginning, in the middle, to the end of the approval process. At the implementation level, this participation must be clear to the user. In this case, electronic media must be able to translate each stage of the process into a user interface model that is easy for users to follow (user-friendly model). In other words, a combination of participation supported by a model-based user interface can be an initial reference in developing the concept of this dynamic consent.

3.6 Characteristics and Formulation of Dynamic Consent in Personal Data Protection

The characteristics of dynamic consent, as implied by its name, are dynamic, providing space for PSE to formulate the concept of dynamic agreement based on the function and feature of each service. Therefore, the form of dynamic consent can be different from other digital media. Dynamic consent can begin to be applied in data processing based on certain scientific activities which will be based on personal data collection. Beyond the scientific scope, the concept of dynamic consent in commercial and governmental PSE is currently under development in many countries.

In Singapore, dynamic consent of PSE application types is under development by The Trust, Transparency and Control Labs (TTC Labs) in collaboration with the Infocomm Media Development Authority (IMDA) under the Singapore Ministry of Information and Technology.[62] Dynamic consent developed within this scope can provide examples of the implementation of dynamic consent in PSE that are deeper than the scientific scope. The elements contained in the scientific scope are almost like a form of agreement. However, the implementation is more interactive and user-friendly.

62 TTC Labs and Infocomm Media Development Authority, "People-Centric Approaches to Notice, Consent, and Disclosure" (Singapore, 2019).

To better understand the difference between the implementation of giving informed consent and dynamic consent, there are at least five differentiating elements, namely: the legitimacy/basis for processing personal data, the approach to Data Subjects/participants/users, the form of giving, the management of giving consent, and the role of authority.[63]

The first element, within the scientific scope, is the legitimacy or basis of dynamic consent processing based on the development of science. Outside the scope of scientific, dynamic consent, personal data is processed on the basis that personal data is an asset that is considered to have economic value for both the Controller and the Data Processor so in the implementation of giving consent, the principles of personal data protection must be observed. The second element, related to the approach to the Data Subject, is in the scientific scope, the Data Subject is the main object known as (participant centric approach). The Controller and Data Processor shall endeavor to accommodate all the needs of the participants by guiding the granting of prior consent via online communication. Meanwhile, outside the scientific scope, Data Subjects are considered PSE users.[64] So, in this case, PSE must try to accommodate users by being aware of the different situations of users.

The third element, the form of giving consent in a scientific scope is not only considered as a default contract written in the T&C and Privacy Policy but can also be in the form of interaction with researchers who will process the Data Subject's personal data.[65] Meanwhile, outside the scientific scope, giving consent is not only in the form of a standard contract written in the Privacy Policy and Terms and Conditions but can also be in the form of interactions with researchers who will process the data subjects' personal data. The fourth element, regarding consent management, in the scientific scope, researchers follow up on the consent given by the Data Subject and provide notification of changes to the processing of personal data and the Data Subject can consider the consent that the user has given through the existing mechanism. Beyond the scientific scope, there is continuous check-in of the consent given by the user. In addition, there is also two-way communication between users and PSE regarding the processing of their personal data.[66]

The fifth element, related to the role of authority, in the scientific scope, in general, the Personal Data Protection Authority (Data Protection Authority) is not directly involved unless there is a complaint about an alleged breach of personal data. Meanwhile, outside the scientific scope, authorities and policymakers are involved in the process of creating dynamic consent prototypes together with technology developers to ensure compliance with personal data protection (co-creation).[67]

Based on the description and examples above, these elements can be drawn to formulate dynamic consent that is right on target and refers to the following: First, it is based on the principle of personal data protection that has been regulated by law. The principles of personal data protection remain the main reference in the formulation of dynamic consent. The dynamic consent formulated by the PSE must comply with the original objective, namely the protection of personal data. These principles are contained in regulations regarding the protection of personal data in each country. Second, consider community practices as data subjects in the field. Apart from being data subjects, the community is also a user of PSE services, both in commercial activities and in government bureaucracy.[68] Therefore, in formulating the right dynamic consent, the behavior of the community as a user is very important to be considered. This is due to the dynamic consent approach which seeks to accommodate community needs; for example by providing an explanation of the Privacy Policy in the form of a video for people with a lower level of understanding of technology. Third, involve existing technological features. There is integration between technological features in PSE services with mechanisms for granting and reviewing approvals. PSE can widen the integration of these technologies by incorporating personal data protection mechanisms as part of the use of the service; for example with pop-up notifications that appear about the use of personal data when users fill out a form. Fourth, involving personal data protection authorities. The dynamic consent formulation engages personal data protection authorities or state policymakers to oversee adherence to the principles of personal data protection from the very beginning of the PSE service.

63 TTC Labs and Infocomm Media Development Authority.
64 TTC Labs and Infocomm Media Development Authority.
65 TTC Labs and Infocomm Media Development Authority.
66 TTC Labs and Infocomm Media Development Authority.
67 TTC Labs and Infocomm Media Development Authority.
68 Djafar, Fadli, and Setianti, *Desain Kebijakan Tata Kelola Konten Internet: Usulan Pelembagaan Dari Perspektif Hak Asasi Manusia*.

The involvement of personal data protection authorities is also inseparable from the existence of the Data Protection Authority (DPA/ Lembaga Pengawas Pelindungan Data Pribadi) as part of enforcing personal data protection laws. The DPA is an institution that has the oversight function of PSE's compliance with the protection of personal data, provides advice and input in the creation of digital services by PSE, and receives public complaints about alleged violations of personal data protection.[69] In addition, the DPA can also carry out the mediation function between the Data Subject and the PSE when there is a dispute regarding data processing, as stipulated by the Singapore Data Protection Act of 2012. In carrying out its functions, the DPA generally has powers, including investigative powers and the imposition of sanctions.[70] In addition, the DPA can also carry out the mediation function between the Data Subject and the PSE when there is a dispute regarding data processing, as stipulated by the Singapore Data Protection Act of 2012. In carrying out its functions, the DPA generally has powers, including investigative powers and the imposition of sanctions.

The elements of dynamic consent that are implemented with the role of the DPA carrying out its functions and powers to the fullest will result in a balance between personal data protection and PSE technological innovation. In addition, the availability of a dispute settlement mechanism related to personal data protection is also needed as PSE's accountability in complying with personal data protection. Personal data dispute resolution mechanisms can be carried out through the DPA or in other forms such as alternative dispute resolution. This provides a broad choice for Data Subjects who suffer losses due to violations committed by PSE to claim their rights. With the implementation of dynamic consent, the participation of the DPA, and an effective dispute-resolution mechanism, the protection of personal data is optimal.

In line with technological developments, the implementation of protection of the right to privacy through personal data protection mechanisms also requires the right approach. The principles contained in the Personal Data Protection regulations have provided guarantees to Data Subjects regarding the use of their Personal Data, provided references to what obligations must be complied with by Data Controllers and Data Processors, as well as the role of the DPA who will oversee the practice of protecting the rights of the privacy. In a special context related to the processing of personal data based on consent by the user or Data Subject, the development of a dynamic consent model can be used as an example of a concrete offer regarding the use of a flexible approach but still in accordance with the principles of personal data protection which prioritizes the Data Subject control over the processing of personal information.

4. Conclusion

Technological developments bring changes in the delivery of services to the public. Various services from the public sector and the private sector have utilized various media (platforms) that can be accessed by both the public. Basically, the working mechanism of the service utilizes the processing of personal data. In processing personal data, there are several bases for processing personal data and one of them is consent from the Data Subject. The majority of services provided by the public and private sectors are consent-based. In practice, the problem that occurs is the emergence of consent overload, which refers to a situation where an individual is given too many requests to give consent or permission regarding the collection and use of personal data. On the other hand, giving excessive consent has consequences for the processing of the Data Subject's personal data which results in further disruption of privacy.

Dynamic consent that is developed within a scientific scope can be used as a reference to answer the consent overload condition. Dynamic consent provides a great deal of flexibility for Data Controllers and Data Subjects. The flexibility in question is that the consent process can be adjusted online by accommodating various media or platforms and taking into account the needs of the Data Subject. Thus, the autonomy of the Data Subject as the holder of control over Personal Data and their privacy is guaranteed while carrying out implementation in accordance with the principles of personal data protection.

There are at least four things that must be combined in formulating dynamic consent as a means of protecting personal data and data subject privacy, namely: First, it is based on the principles of personal data protection that

69 Wahyudi Djafar and M. Jodi Santoso, "Pelindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen," *Lembaga Studi Dan Advokasi Masyarakat, Seri Internet Dan HAM*, 2019, 2.

70 David Erdos, "Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?," *Cambridge Faculty of Law Research Paper No. 14/2020*, 2020.

have been regulated by law. Second, consider community practices as data subjects in the field (participant-centric approach). Third, use existing technological features by prioritizing interaction and communication between Data Subjects and Data Controllers as reflected in the Privacy Policy. And fourth, the involvement of the Personal Data Protection Authority as a guarantee of the Data Controller's compliance in carrying out the principles of personal data protection.

ACKNOWLEDGMENTS

The authors express our gratitude to the Pusat Studi Hukum dan HAM (Center of Human Rights and Law Studies/HRLS) Faculty of Law, Airlangga University, HRLS researchers for their constructive suggestions during the process of compiling this article.

BIBLIOGRAPHY

Arief, Verdico. "E-Government Di Asia Tenggara: Perbandingan Pengembangan E-Government Di Singapura, Malaysia Dan Indonesia." *Social Issues Quarterly* 1, no. 2 (2023): 345–62.

Bester, Johan, Cristie M. Cole, and Eric Kodish. "The Limits of Informed Consent for an Overwhelmed Patient: Clinicians' Role in Protecting Patients and Preventing Overwhelm." *AMA Journal of Ethics* 18, no. 9 (2016): 869–86. https://doi.org/10.1001/journalofethics.2016.18.9.peer2-1609.

Brockdorff, N.; Appleby-Arnold, S. "What Consumers Think." *EU Consent Project*, 2015.

Buchner, Benedikt, and Merle Freye. "Informed Consent in German Medical Law: Finding the Right Path between Patient Autonomy and Information Overload." In *SSRN Electronic Journal*, 2022. https://doi.org/10.2139/ssrn.4088631.

Budin-Ljøsne, Isabelle, Harriet J.A. Teare, Jane Kaye, Stephan Beck, Heidi Beate Bentzen, Luciana Caenazzo, Clive Collett, et al. "Dynamic Consent: A Potential Solution to Some of the Challenges of Modern Biomedical Research." *BMC Medical Ethics* 18, no. 1 (2017): 1–10. https://doi.org/10.1186/s12910-016-0162-9.

Bygrave, Lee A. "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties." *International Journal of Law and Information Technology*, 1998, 4.

Djafar, Wahyudi, Miftah Fadli, and Lintang Setianti. Desain Kebijakan Tata Kelola Konten Internet: Usulan Pelembagaan Dari Perspektif Hak Asasi Manusia, 2017.

Djafar, Wahyudi, and M. Jodi Santoso. "Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen." *Lembaga Studi Dan Advokasi Masyarakat, Seri Internet Dan HAM*, 2019, 2.

Dove, Edward S., and Jiahong Chen. "Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis." *International Data Privacy Law*, 2020.

Elde, Asbjorn, Alfredsson Gudmundur, and Göran Melander. *The Universal Declaration of Human Rights: A Commentary*. Oslo: Scandinavian University Press, 1992.

Erdos, David. "Accountability and the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?" *Cambridge Faculty of Law Research Paper No. 14/2020*, 2020.

Firdaus, Indriana. "Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan." *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 4, no. 2 (2022): 23–31. https://doi.org/10.52005/rechten.v4i2.98.

Government, Digital. "E-Government Survey 2022." New York, 2022.

Guidelines, Advisory, O N Requiring, Consent For, and Marketing Purposes. "Advisory Guidelines on Requiring Consent for Marketing Purposes." Singapore, 2015.

Hern, Alex. "Facebook Usage Falling after Privacy Scandals, Data Suggests." *The Guardian*, June 2019.

Human Rights Committee General Comment. "On the Right To Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation." Vol. I, 2013.

Indonesia, Badan Pusat Statistik Republik. "Statistik E-Commerce 2022." Jakarta, 2022.

Indonesia, CNN. "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah." Accessed March 16, 2023. https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah.

Indriani, Masitoh, and Ekawestri Prajwalita Widiati. "The Privacy Challenge in the 'Smart Era': A Study of the Implementation of e-Government in Surabaya." *ICPS 2018 Proceeding*, no. Icps (2019): 641–44. https://doi.org/10.5220/0007548606410644.

Internet Society. "Global Internet Survey, Summary Report," n.d.

Jayawickrama, Nihal. The Judicial Application of Human Rights Law, National, Regional and International Jurisprudence. Cambridge: Cambridge University Press, 2002.

Kaye, Jane, Edgar A. Whitley, David Lund, Michael Morrison, Harriet Teare, and Karen Melham. "Dynamic Consent: A Patient Interface for Twenty-First Century Research Networks." *European Journal of Human Genetics* 23 (2015): 3.

Kurbalija, Jovan. An Introduction to Internet Governance. Diplo Foundation. Diplo Foundation, 2014.

Lister, John. "Privacy Policies Are Legally Required." Accessed March 16, 2023. https://www.freeprivacypolicy.com/blog/privacy-policy-legally-required/.

Malik, Abdul. "Survei OJK 2022 : Inklusi Keuangan Naik Jadi 85,1% Dan Literasi 49,6%." Accessed March 16, 2023. https://www.bareksa.com/berita/pasar-modal/2022-10-30/survei-ojk-2022-inklusi-keuangan-naik-jadi-851-dan-literasi-496.

Masyhur, Firdaus. "Penelitian E-Government Di Indonesia: Studi Literatur Sistematis Dari Perspektif Dimensi Pemeringkatan e-Government Indonesia (PeGI)." *JURNAL IPTEKKOM : Jurnal Ilmu Pengetahuan & Teknologi Informasi* 19, no. 1 (2017): 51. https://doi.org/10.33164/iptekkom.19.1.2017.51-62.

Rahayu, Isna Rifka Sri. "Hasil Survei: Promosi Tak Lagi Jadi Penentu Utama Pilih e-Commerce." Accessed March 16, 2023. https://money.kompas.com/read/2022/12/08/171000026/hasil-survei--promosi-tak-lagi-jadi-penentu-utama-konsumen-pilih-e-commerce?page=all.

Rahman, Faiz, and Dian Agung Wicaksono. "Researching References on Interpretation of Personal Data in the Indonesian Constitution." *Jurnal Penelitian Hukum De Jure* 21, no. 2 (2021): 187. https://doi.org/10.30641/dejure.2021.v21.187-200.

Razaghpanah, Abbas, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, and Phillipa Gill. "Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem." In *Proceedings 2018 Network and Distributed System Security Symposium*. Reston, VA: Internet Society, 2018. https://doi.org/10.14722/ndss.2018.23353.

Rizkinaswara, Leski. "Gerakan Menuju 100 Smart City." Accessed March 16, 2023. https://aptika.kominfo.go.id/2022/07/gerakan-menuju-100-smart-city-2/.

Rosadi, Sinta Dewi. "Perlindungan Data Pribadi Sebagai Alat Utama Menjamin Hak Privasi Warga Negara." *Kebebasan Berekspresi Di Indonesia: Hukum, Dinamika, Masalah Dan Tantangannya*, 2016, 210.

Saefudin. "Signifikan, Hasil Survei e-Government Indonesia Naik 11 Peringkat." Accessed March 16, 2023. https://aptika.kominfo.go.id/2022/10/signifikan-hasil-survei-e-government-indonesia-naik-11-peringkat/.

Schermer, Bart W., Bart Custers, and Simone Van der Hof. "The Crisis of Consent." *Ethics and Information Technology*, no. 2007 (2014): 1–19. https://doi.org/10.1007/s10676-.

Schlehahn, Eva, Patrick Murmann, and Farzaneh Karegar. "Opportunities and Challenges of Dynamic Consent in Commercial Big Data Analytics." In *IFIP International Summer School on Privacy and Identity Management*, 29–44. Springer, 2020. https://doi.org/https://doi.org/10.1007/978-3-030-42504-3_3.

Sugiyanti, Umi, and Agung Pambudi. "Perlindungan Data Privasi Dan Kebebasan Informasidalam Platform WhatsApp." *Jurnal IPI (Ikatan Pustakawan Indonesia* 7, no. 2 (2022): 60–70.

Surfshark Lab. "Data Breaches Rise Globally in Q3 of 2022." Data breaches rise globally in Q3 of 2022. Accessed March 16, 2023. https://surfshark.com/blog/data-breach-statistics-2022-q3.

Teare, Harriet J.A., Megan Prictor, and Jane Kaye. "Reflections on Dynamic Consent in Biomedical Research: The Story so Far." *European Journal of Human Genetics* 29, no. 4 (2021): 649–56. https://doi.org/10.1038/s41431-020-00771-z.

the European Commission. "Opinion 15/2011 on the Definition of Consent." Opinion 15/2011 on the definition of consent. Accessed March 16, 2023. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

the United Nations. "The United Nation E-Government Survey 2022: The Future of Digital Government." New York, n.d. https://desapublications.un.org/sites/default/files/publications/2022-09/Web version E-Government 2022.pdf.

Tirah Arum Toewoeh. "Kominfo Gerak Cepat Tangani Lima Kasus Baru Kebocoran Data." Kementerian Komunikasi dan Informatika RI. Accessed March 16, 2023. https://aptika.kominfo.go.id/2022/11/kominfo-gerak-cepat-tangani-lima-kasus-baru-kebocoran-data.

TTC Labs, and Infocomm Media Development Authority. "People-Centric Approaches to Notice, Consent, and Disclosure." Singapore, 2019.

UK Information Commissioner's Office. "Guide to the General Data Protection Regulation," 2019.

Warren, Samuel D, and Louis D Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193–220. https://doi.org/10.2307/1330091.

Westin, Alan F. *Privacy and Freedom*. New York: Atheneum Press, 1967.

Wirawan, Vani. "Penerapan E-Government Dalam Menyongsong Era Revolusi Industri 4.0 Kontemporer Di Indonesia." *Jurnal Penegakan Hukum Dan Keadilan* 1, no. 1 (2020): 1–16. https://doi.org/10.18196/jphk.1101.

Working Party 29. "Opinion 15/2011 on the Definition of Consent," 2011.

Undang-Undang Dasar 1945 (1945).

Undang-Undang No. 12 Tahun 2005 entang Pengesahan International Covenant on Civil and Political Rights (Kovenan Internasional Tentang Hak-Hak Sipil dan Politik), § Lembaran Negara Republik Indonesia Tahun 2005 Nomor 119 (2008).

Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, § Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58 (2008).

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, § Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251 (2016).

Undang-Undang Republik Indonesia No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, § Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196 (2022).

Universal Declaration of Human Rights (1948).

Author Statement:

Author Contribution - Masitoh Indriani: *first author, correspondence author.* **Annida Aqiila Putri:** *second author.*

Conflict of Interest - The authors of this journal declare that there is no conflict of interest.

Originality of Research - The authors of this journal declare that this journal is the original work of the authors, this journal is also free of plagiarism, has included references, and this journal has never been published and has never been submitted to another journal.

Sponsorship – The writing of this journal is supported by funding from RKAT Airlangga University.