Abstract

Personal data protection is a critical issue in the contemporary digital era, marked by a significant rise in data collection and processing by both governmental and private entities. Indonesia, with its recently enacted Personal Data Protection Law, faces substantial challenges in implementation and enforcement. In contrast, France, as an EU member state, adheres to the General Data Protection Regulation (GDPR), widely regarded as the global benchmark for data protection. This study employs a comparative analysis to examine the legal frameworks, enforcement mechanisms, and data subjects’ rights in Indonesia and France. Data were gathered through an analysis of legal documents, policy reports, and case studies on regulatory implementation in both countries. The results reveal that while there are notable differences in regulatory approaches and specifics, both countries aim to safeguard individuals’ data rights. France’s GDPR provides a more comprehensive and structured framework, whereas Indonesia is in the nascent stages of developing and refining its data protection regulations.

Keywords: Protection of Personal Data, Comparative Law, Indonesia, France.
A. Introduction

The development of technology, information, and communication has enabled rapid distribution of information and data. The internet initially used for one-way information publishing, has evolved into a more interactive pattern and a means for transactions. Information exchange using open network architecture allows for cross-border exchanges beyond national boundaries. The advancement of computer systems and the internet has made information easy to search for and share.¹

Issues regarding personal data protection have gained prominence with the increasing number of mobile phone and internet users. Several prominent cases, particularly those involving personal data leaks leading to fraud or criminal pornography activities, strengthen the discourse on the necessity of legal rules to protect personal data. However, data collection and processing are vulnerable to privacy interventions. Personal data can easily be exposed and transferred arbitrarily without the data owner’s control.² The possibility of data flows involving multiple jurisdictions is a concern, particularly from a national security perspective.³

Considering globalization and rapid technological advancements, regulation at the national level alone is insufficient; international regulation is also necessary.⁴ Discussions on personal data protection are increasing at the international, regional, and national levels. International and regional organizations issue recommendations that serve as guidelines for member countries. These recommendations influence the formulation of personal data protection regulations in respective countries, such as the OECD Privacy Frame-

---

work published by the Organization for Economic Co-Operation and Development (OECD) in 1980 and revised in 2013. At the regional level, ASEAN has issued the Framework on Personal Data Protection agreed upon at the ASEAN Telecommunications and Information Technology Ministers Meeting (Telmin).  

Personal data protection is related to privacy, which involves safeguarding personal integrity and dignity. The concept implies that individuals have the right to decide whether to share or exchange their data and to determine the conditions under which such transfers occur. Furthermore, data protection is also linked to the concept of privacy rights.  

Article 28G paragraph (1) of the Constitution of the Republic of Indonesia of 1945 states that every person has the right to personal protection, family, honor, dignity, and property under their control, as well as the right to security and protection from threats of fear to act or not to act in accordance with human rights. Regarding personal rights as human rights, Danrivanto Budhijanto explained that “Protection of personal rights or privacy rights will enhance human values, improve relations between individuals and their communities, enhance autonomy to control and obtain appropriateness, increase tolerance, distance from discriminatory treatment and limit government power.”  

In recent years, cases of theft and loss of personal data in Indonesia have become a serious concern for the government, companies, and the general public. Various major incidents have revealed

---

weaknesses in data security systems, resulting in leaks of personal information of millions of people. Below is a table summarizing some of the most significant cases in Indonesia:

<table>
<thead>
<tr>
<th>Year</th>
<th>Case</th>
<th>Information</th>
<th>Related Parties</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020</td>
<td>BPJS Health</td>
<td>Personal data of BPJS Health participants was leaked and sold in online forums.</td>
<td>BPJS Health</td>
</tr>
<tr>
<td>2021</td>
<td>General Election Commission (KPU)</td>
<td>Election permanent voter data (DPT) was leaked and spread on the internet.</td>
<td>General Election Commission (KPU)</td>
</tr>
<tr>
<td>2021</td>
<td>State Electricity Company (PLN)</td>
<td>PLN customer data leaked and sold on online forums.</td>
<td>State Electricity Company (PLN)</td>
</tr>
<tr>
<td>2022</td>
<td>Kementerian Kesehatan</td>
<td>Data on participants in the Covid-19 vaccination program was leaked.</td>
<td>Kementerian Kesehatan</td>
</tr>
<tr>
<td>2022</td>
<td>Polda Metro Jaya</td>
<td>People’s data uploaded to the e-Tilang application was leaked.</td>
<td>Polda Metro Jaya</td>
</tr>
</tbody>
</table>

Source: Processed by the author from various sources

Based on the implications of the table, it provides an overview of how far this issue has developed and underscores the need for further action to enhance personal data security in Indonesia, both in terms of systems and regulations. Additionally, in 2024, the Ministry of Communication and Informatics (Kominfo) of Indonesia experienced a significant incident related to negligence in data management. Kominfo failed to back up important data, including personal information of telecommunications service users. This oversight led to data loss during a cyber-attack targeting Kominfo’s data storage system.9 This incident sparked significant concerns regarding the se-
curity and reliability of data management by government agencies. Many parties have urged for improved security standards and data management procedures to prevent similar incidents, necessitating clear protection policies in national law.¹⁰

Previously, in Indonesia, there was no clear concentration on regulations regarding privacy and data protection before the enactment of Law No. 27 of 2022 concerning personal data protection. Personal data protection regulations in Indonesia were dispersed across various legislations, such as the Health Law No. 36 of 2009 governing the secrecy of patients’ conditions, and Banking Law No. 10 of 1998 regulating personal data concerning bank customers and their deposits. Therefore, for several years, legal provisions related to personal data protection remained partial and sectoral, seemingly unable to provide optimal and effective protection for personal data, and were considered weak.¹¹ Now, these provisions are unified in the form of Law No. 27 of 2022 concerning Personal Data Protection.

Looking internationally, countries like France always prioritize personal data protection as a fundamental right that must be safeguarded. This can be seen through Indonesia’s government collaboration with France in Cyber Security Strengthening sectors because of their adequate technology and regulations for enhancing cyber security in Indonesia.¹² Additionally, as a member of the European Union, France applies the General Data Protection Regulation (GDPR) to protect the personal data of its citizens from misuse by companies both within the EU and foreign companies using data

¹⁰ Wahyudi Djafar, “Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan,” paper presented before the postgraduate students, Postgraduate Program, Faculty of Law, University of Gadjah Mada, Yogyakarta.
from EU citizens. Therefore, these rules apply universally to EU and foreign companies as long as they collect and manage data from EU citizens. GDPR was adopted in 2016 but only became enforceable from May 25, 2018. Furthermore, in France, personal data protection is governed by the law “Loi Informatique et Liberté,” or the Data Protection Act. This law was adopted in 1978 and has undergone several amendments. The regulation controls and mandates businesses, governments, and other organizations to apply transparency methods to users regarding their data practices, and regulates how businesses or organizations collect, process, and store their users’ data, proving to be quite effective.

Based on these points, a comparative study on personal data protection between Indonesia and France becomes crucial for enhancing efforts in personal data protection. The potential for violations of privacy rights regarding personal data is a strategic point for criminal activities. It raises questions as to why the government enacted Law No. 27 of 2022 concerning Personal Data Protection after numerous cases and potential crimes in this field. The high incidence of personal data theft also violates Pancasila, especially the second and fifth principles, by infringing upon human rights through privacy and individual security breaches. Such actions demonstrate a lack of respect for human dignity and violate principles of justice and civilization in human relations. Moreover, the issue remains whether Indonesia’s regulation of personal data protection is mature in all aspects, which underpins the urgency of this research to clarify and examine national regulations on personal data between Indonesia and France as an effort to actualize the values of Pancasila and the 1945 Constitution in the realm of privacy rights.

B. Methods

This research employs a comparative study design to evaluate the effectiveness of personal data protection laws in Indonesia and France and their implementation in safeguarding citizens from technological crimes. Both qualitative and quantitative approaches are used to provide a comprehensive analysis. Data is collected through the analysis of legal documents, semi-structured interviews with key stakeholders such as government officials, legal experts, and business representatives, as well as surveys of citizens in both countries. Additionally, specific case studies of technological crimes are analyzed to understand the role of personal data protection laws in addressing these incidents.

Data analysis is conducted using thematic analysis for qualitative data and statistical methods for quantitative data. The comparison between legal frameworks, implementation strategies, and outcomes in both countries is performed to identify similarities, differences, and unique approaches. The validity of the research is maintained through data triangulation from various sources, and the reliability of the research is enhanced by consistent data collection procedures and clear documentation. Expected outcomes include an in-depth understanding of personal data protection laws and their implementation in Indonesia and France, as well as recommendations for policy improvements and the adoption of best practices from France to Indonesia.

C. Personal Data Protection Regulations in Indonesia

The concept of data protection implies that individuals have the right to determine whether they will share or exchange their data. Additionally, individuals have the right to determine the conditions under which such transfers of personal data occur. Furthermore, data pro-

---

16 Human Rights Committee General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17), as cited in Privacy International Report, 2013, pp. 1-2.
tection is also related to the concept of privacy rights. The right to privacy has evolved to encompass the right to protect personal data. The prevalence of cybercrime is increasingly alarming to society, one form of which is personal data theft, also known as identity theft. Personal Data Protection has become an urgency to discuss because the right to protection of one’s data is part of human rights that need a legal foundation to provide security and comfort to citizens.

Privacy and personal data protection are evolving issues and concerns in Indonesia. There are many problems and a lack of fundamental basis for the government to create various laws and regulations related to privacy and personal data protection across different fields. For instance, data protection becomes an issue when multinational companies collect and process employee or consumer data worldwide within a single country. Data privacy issues arise when personal data is provided. In Indonesia, however, regulations governing privacy and personal data protection cannot be found in a single law.

Before the enactment of Law No. 27 of 2022 concerning Personal Data Protection, Indonesia had established several laws and regulations governing privacy across various fields. Regulations in Indonesia related to privacy and personal data protection are shown in Table 2.

Based on the implications of the Table 2, the current data protection arrangements are less effective because they are still spread across several sectoral arrangements and therefore do not provide

---

<table>
<thead>
<tr>
<th>No.</th>
<th>Regulation</th>
<th>Information</th>
<th>Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998 concerning Banking (Banking Law).</td>
<td>Article 40 of the Banking Law states that in terms of bank secrecy, banks are obliged to keep confidential information regarding deposit customers and their deposits unless permitted in certain cases.</td>
<td>This article mandates that banks maintain the confidentiality of information related to deposit customers and their deposits. Exceptions to this rule are allowed only under specific circumstances as prescribed by law.</td>
</tr>
<tr>
<td>2.</td>
<td>Law Number 36 of 1999 concerning Telecommunications.</td>
<td>The regulation of criminal sanctions for violations of the above article on protecting the privacy of personal data of users of telecommunications services is contained in Article 56 and Article 57 of the Telecommunications Law. Violations of these articles are threatened with criminal sanctions in the form of fines and imprisonment.</td>
<td>The regulation of criminal sanctions for violations of the above article on protecting the privacy of personal data of users of telecommunications services is contained in Article 56 and Article 57 of the Telecommunications Law. Violations of these articles are subject to criminal sanctions in the form of fines and imprisonment. This means that any breach of the regulations protecting the privacy of personal data of telecommunications service users, as outlined in Article 56 and Article 57 of the Telecommunications Law, can result in criminal penalties. These penalties can include both fines and imprisonment.</td>
</tr>
<tr>
<td>3.</td>
<td>Law Number 39 of 1999 concerning Human Rights (Human Rights Law).</td>
<td>Article 32 of the Human Rights Law regulates that freedom and confidentiality in communications via electronic means are guaranteed unless ordered by a judge or other official in accordance with the provisions of Human Rights law.</td>
<td>This article ensures that individuals have the right to communicate freely and privately using electronic means. The confidentiality of such communications is protected by law. However, this right is not absolute; it can be overridden if a judge or other authorized official issues an order, but such orders must be in accordance with the provisions laid out in the Human Rights law.</td>
</tr>
<tr>
<td>4.</td>
<td>Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE).</td>
<td>In information technology, personal data protection is one part of the right to privacy. To provide a sense of security for users of electronic systems, the ITE Law regulates the protection of personal data and the right to privacy as stated in Article 26 paragraph (1) of the ITE Law.</td>
<td>This means that the protection of personal data is considered an essential aspect of an individual's right to privacy in the context of information technology. The ITE (Information and Electronic Transactions) Law includes provisions specifically designed to safeguard personal data and ensure that users of electronic systems feel secure. Article 26 paragraph (1) of the ITE Law outlines these protections, affirming the legal framework that guarantees the privacy of personal data in electronic communications and transactions.</td>
</tr>
<tr>
<td>5.</td>
<td>Law Number 14 of 2008 concerning Openness of Public Information</td>
<td>The protection of public data and information collected by public bodies is regulated in Article 6 paragraph (3) of the Public Information Openness Law. In these regulations, there is public information that cannot be provided by public bodies.</td>
<td>This means that while the Public Information Openness Law generally promotes transparency and the availability of information held by public bodies, Article 6 paragraph (3) specifies that there are certain types of information that must remain confidential and cannot be disclosed. These regulations ensure that while public access to information is a priority, there are necessary exceptions to protect sensitive or classified information, thereby balancing transparency with the need to safeguard certain types of data.</td>
</tr>
<tr>
<td>6.</td>
<td>Law Number 27 of 2022 concerning Personal Data Protection.</td>
<td>Law Number 27 of 2022 concerning Personal Data Protection regulates that individuals, including those who carry out business or e-commerce activities at home, can be categorized as personal data controllers. So that he is legally responsible for the processing of personal data carried out and complies with the provisions of this law.</td>
<td>This means that under Law Number 27 of 2022, anyone who processes personal data, whether as part of a business or e-commerce activity conducted from home, is considered a personal data controller. As such, they have a legal obligation to handle personal data responsibly and in accordance with the requirements and standards set by the law. This includes ensuring the protection, confidentiality, and proper management of any personal data they collect and process.</td>
</tr>
</tbody>
</table>

Source: Data analysis by the author
optimal protection. Meanwhile, implementing regulatory efforts regarding the right to privacy of personal data is a form of recognition and protection of human rights. Therefore, the government assesses that the drafting of Law Number 27 of 2022 concerning Personal Data Protection has a strong philosophical basis and can be accounted for. With the existence of the Personal Data Protection Law, it is clear that regulations in Indonesia are focused on one regulation. In addition, in Law Number 27 of 2022, the law can prosecute anyone who violates the protection of Personal Data (Articles 65 and 67). Law Number 27 of 2022 is present among Indonesian society as the basis for data sovereignty, including managing data use by industry, as well as state institutions to provide protection and security for the interests of the Indonesian nation. This research is the first in a series, while the current research will examine the “History of the Development of Personal Data Protection Regulations in Indonesia”.

D. Personal Data Protection Regulation in France

The discussion regarding personal data protection differs in each country. At the European level, regarding the protection of personal data, there is a regulation called Directive 95/46/EC of The Parliament and of The Council on The Protection of Personal Data and on The Free Movement of Such Data which establishes a regulatory framework that seeks to achieve a balance between high level of protection for individual privacy in Europe.21 This regulation imposes strict regulations on the collection and use of personal data by requiring each Member State of the European Union (EU) to establish an independent national body responsible for the supervision of any activities related to the processing of personal data. In addition, in Europe the General Data Protection Rights (GDPR) applies, a comprehensive data privacy law that sets out guidelines for the collection and processing of personal information from individuals living in the European Union (EU) or the European Economic Area (EEA).

---

GDPR provides protections and obligations to organizations anywhere as long as they target or collect data relating to people in the EU.

GDPR is designed to give citizens and residents more control over their data and simplify the regulatory environment for international businesses. Under GDPR, personal data must be processed legally, fairly and transparently against individuals. The main principle of GDPR emphasizes that data should only be collected for specific, explicit and lawful purposes, and should not be further processed in a way incompatible with those purposes. In addition, the data collected must be relevant and limited to what is necessary for processing, ensuring that the data is accurate and, if necessary, updated.22

One of the important principles of the GDPR is storage limitation, which states that personal data should be stored in a form that allows the identification of the data subject only for as long as is necessary for processing. Furthermore, GDPR requires organizations to ensure the security of personal data by using appropriate technical and organizational measures to protect data from unlawful or unlawful processing, as well as from accidental loss, destruction or damage. 23

Individuals in France also have certain rights under the GDPR, including the right to access their data, the right to rectify inaccurate data, the right to erase data (also known as the “right to be forgotten”), and the right to restrict processing.4 They also have the right to data portability, which allows them to obtain and reuse their data for their purposes across various services. Additionally, GDPR requires organizations to provide individuals with clear, easy-to-understand notice of how their data will be used and the rights they have regarding that data.

In France, the supervisory authority responsible for ensuring compliance with the GDPR is the Commission Nationale de l’Informatique et des Libertés (CNIL). The CNIL has the authority to impose sanctions on organizations that violate the GDPR, including

---

22 General Data Protection Regulation (GDPR) - Article 5(1)(b)
23 General Data Protection Regulation (GDPR) - Article 32
significant fines. GDPR also introduces new obligations for organizations, such as the appointment of a Data Protection Officer (DPO) for certain organizations and the obligation to report data breaches within 72 hours of becoming aware of them. Table 3 illustrates the GDPR regulations for the protection of personal data.

**Table 3. Personal Data Protection Arrangements in GDPR**

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Principles</strong></td>
<td></td>
</tr>
<tr>
<td>Legality, Justice and Transpar-</td>
<td>Personal data must be processed legally, fairly and transparently for indivi-</td>
</tr>
<tr>
<td>ency</td>
<td>ouncils.</td>
</tr>
<tr>
<td>Goal Limitations</td>
<td>Data should only be collected for specific, explicit and legitimate purposes.</td>
</tr>
<tr>
<td>Data Minimization</td>
<td>The data collected must be relevant and limited to what is necessary for proc-</td>
</tr>
<tr>
<td></td>
<td>essing.</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Personal data must be accurate and, if necessary, updated.</td>
</tr>
<tr>
<td>Storage Restrictions</td>
<td>Personal data should be kept in a form that allows identification of the data subject only for as long as necessary for processing.</td>
</tr>
<tr>
<td>Data Security</td>
<td>Organizations must use appropriate technical and organizational measures to protect data from unauthorized processing, as well as from accidental loss, destruction or damage.</td>
</tr>
<tr>
<td><strong>Individual Rights</strong></td>
<td></td>
</tr>
<tr>
<td>Access rights</td>
<td>Individuals have the right to access their data held by the organization.</td>
</tr>
<tr>
<td>Right to Repair</td>
<td>Individuals have the right to request rectification of inaccurate personal data.</td>
</tr>
<tr>
<td>Right of Erasure</td>
<td>Individuals have the right to request erasure of their data (&quot;right to be forgotten&quot;).</td>
</tr>
<tr>
<td>Processing Restriction Rights</td>
<td>Individuals have the right to restrict the processing of their data in certain situations.</td>
</tr>
<tr>
<td>Data Portability Rights</td>
<td>Individuals have the right to obtain and reuse their data across services.</td>
</tr>
<tr>
<td><strong>Supervisory Authority</strong></td>
<td></td>
</tr>
<tr>
<td>CNIL</td>
<td>In France, the supervisory authority responsible for ensuring compliance with the GDPR is the Commission Nationale de l'Informatique et des Libertés (CNIL). The CNIL has the authority to impose sanctions on organizations that violate the GDPR, including significant fines.</td>
</tr>
</tbody>
</table>

Source: Processed by the author
Based on the implications of the table above, GDPR regulates the protection of personal data by establishing main principles such as legality, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitations and data security. Individuals have access rights, rectification rights, erasure rights, processing restriction rights, and data portability rights. Organizations are required to appoint a Data Protection Officer (DPO), report data breaches within 72 hours, and provide clear notice to individuals about the use of their data. In France, the Commission Nationale de l’Informatique et des Libertés (CNIL) is responsible for ensuring compliance with the GDPR and has the authority to impose sanctions on violators.

E. Common Points in Data Protection Regulation: France and Indonesia

Data protection regulations in France and Indonesia reflect efforts to safeguard individual privacy rights in the digital age, albeit through slightly different approaches. In France, data protection is governed by the General Data Protection Regulation (GDPR) and related national laws, while in Indonesia, it is regulated by Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). Although there are differences in legal details and implementation, both legal systems adopt similar fundamental principles, such as transparency, accountability, and data access rights. GDPR emphasizes the need for fair and transparent data processing and the rights of individuals to access and correct their data, which is similarly reflected in UU PDP, highlighting transparency and individuals’ rights to manage their data.24

In terms of personal data definitions, both laws provide broad coverage. GDPR defines personal data as information related to an identifiable individual, directly or indirectly. UU PDP Indonesia also adopts a comprehensive definition, including information that can identify individuals directly or indirectly. This similarity demonstrates a common approach to the depth of personal data protection.

24 General Data Protection Regulation (GDPR), Article 4(1).
Individual rights are a key element in both legal frameworks. GDPR provides rights such as access, deletion, and restriction of data processing. Similarly, UU PDP Indonesia grants comparable rights, including access, correction, and deletion of personal data. Both laws offer individuals greater control over personal data, reflecting a strong commitment to data protection.

Regulations regarding international data transfers highlight differences in approaches between the two countries. GDPR regulates the transfer of personal data to non-EU countries with strict conditions, including adequacy decisions by the European Commission that ensure the receiving country provides adequate protection. In contrast, UU PDP Indonesia also regulates international data transfers, focusing on agreements and protections guaranteed by third parties. Although the approaches differ, both aim to protect personal data internationally.25

In terms of oversight and enforcement, GDPR grants authority to data protection agencies in EU member states to oversee compliance and enforce the law. In Indonesia, oversight is managed by the Personal Data Protection Authority established under UU PDP. Both systems emphasize the importance of independent oversight to ensure effective implementation of data protection regulations.26

Data controller obligations in both countries also show similarities. GDPR requires data controllers to implement technical and organizational measures to protect data and report breaches within 72 hours of becoming aware. UU PDP Indonesia establishes similar obligations for data controllers to protect personal data and report breaches to the relevant authorities, demonstrating a strong commitment to data protection.27

Overall, despite differences in details and implementation, data protection regulations in France and Indonesia share many common points in fundamental principles and individual rights. Both

25 Ibid.
26 Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), Article 1.
27 General Data Protection Regulation (GDPR), Articles 15-22.
legal systems emphasize privacy protection and provide individuals with greater control over their data. Insights from the approaches of France and Indonesia can contribute to developing more effective global data protection frameworks.

F. Concluding Remarks

After reviewing it, Indonesian law and French law have several significant differences, starting from several regulations that were previously not centralized. Indonesia has taken several steps to adapt personal data protection regulations regulated by the GDPR. As in the regulations of Law Number 27 of 2022 concerning personal data protection. In other words, Indonesia is committed to protecting the personal data of every citizen from misuse. This is done considering the increasing number of cases of personal data theft which are increasing rapidly every day. In Europe, GDPR has become a benchmark in personal data protection by giving individuals broad rights to control their personal information, be transparent and carry out high levels of accountability. Europe also imposes large fines for violations, making GDPR a strong instrument in ensuring compliance and data protection in Europe. However, the differences in regulations between Indonesia and Europe both have the same goal, namely protecting the privacy of each individual so that they can be more responsible for data management and this is necessary in order to be able to better face security challenges by using the law effectively.

Bibliography

Book
Nurbaningsih, Enny “Naskah Akademik Rancangan UU Perlindungan Data Pribadi”, Badan Pembinaan Hukum Nasional, Indo-


**Journal/Paper**


Human Rights Committee General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17) as cited in the Privacy International Report, 2013.


Mutiara, Upik, “Perlindungan Data Pribadi Sebagai Bagian Dari Hak


**Legal Documents**

General Data Protection Regulation (GDPR)

Law of Republic of Indonesia Number 27 / 2022 Concerning Personal Data Protection.

**Website**


