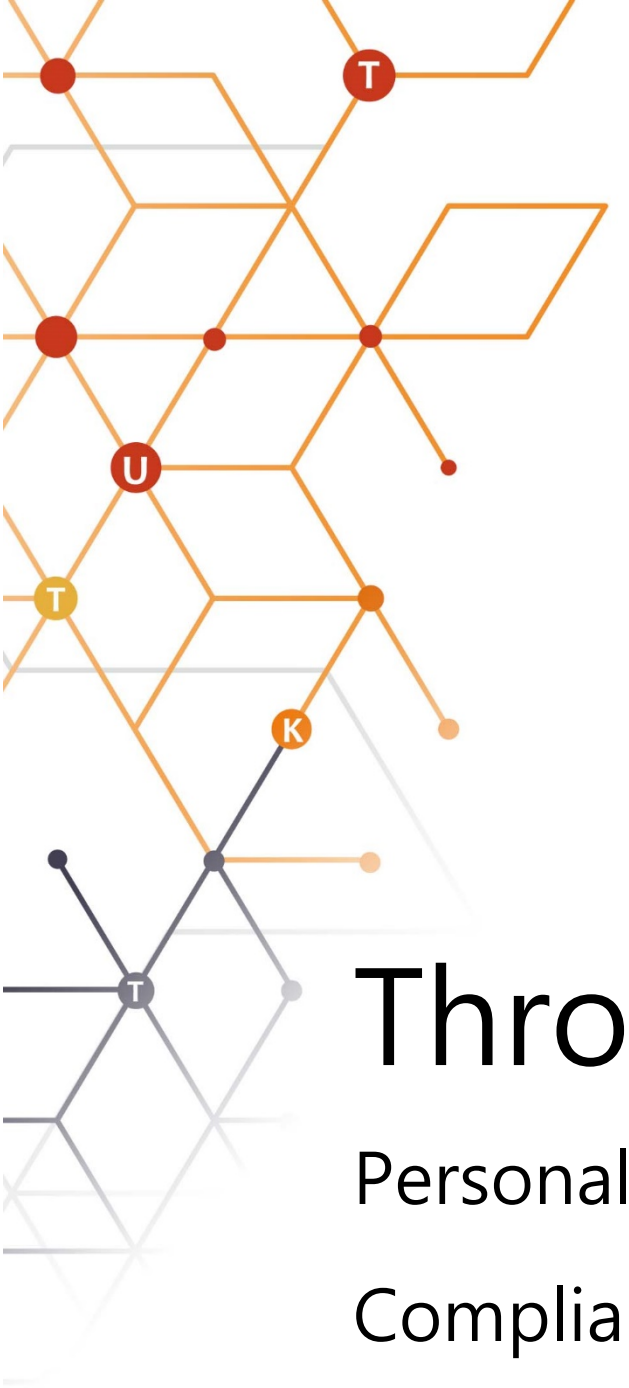

物聯智慧股份有限公司
ThroughTek Co., Ltd.

ThroughTek -

Personal Data Protection Compliance White Paper

How to Strengthen Personal Data Protection According to GDPR.

2018/6

1. Introduction

2. Our Commitment to Data Privacy Protection

3. Our Understanding of GDPR

4. Our Work on GDPR Compliance

5. Data Privacy Protection Technology Challenges

6. Conclusion

1. Introduction

Everyone wants their personal data to be reasonably used by government agencies and business organizations, and not to be exploited, shared, or sold to any third party for profit or other purposes without consent. Most importantly is that you have full control over all information that belongs to your privacy, and you decide for yourself who can receive your personal information, how it is used, and when it is transferred or deleted. In this technological age, this growing demand for data privacy protection have been expressed by more and more people, and has gradually been reflected in the requirements of relevant laws in various countries. The EU General Data Protection Regulation (GDPR), which takes effect on May 25, 2018, establishes a new set of global standards for the privacy and security of personal data. This new regulation is applicable to most multinational corporations, especially profit and non-profit organization in the Internet of Things ecosystem, and with or without a presence in the European Union.

Throughtek is highly committed to the universal value of data privacy protection and has promoted a series of transformations of organizational processes and product design through GDPR compliance preparation. We hope to continuously improve data privacy protection and achieve our commitment. At the same time, we are happy to share our experiences and cooperate with our customers to help them meet the standards placed by GDPR.

2. Our Commitment to Data Privacy Protection

In order to meet the requirements of GDPR, we worked closely with internal and external experts, safety and security agencies and

professional consultants. We also referred to the EU's official authorities, the EU's major member countries and international associations, such as IAPP and CISPE, compliance guides and work lists, to help us plan and promote all necessary actions and procedures to protect personal data privacy. Additionally, we prioritize the implementation of GDPR compliance measures to European related businesses, and will continue to gradually adjust the same data privacy protection standards for operational activities and product services in other regions.

Since the establishment of Throughtek, we have always been a benchmark for the industry, providing audio/video applications and P2P connection services while protecting personal data privacy, because respecting the privacy of users is the upmost importance of our core corporate culture. Therefore, despite the high cost of data privacy protection measures, we strive to work together with customers and suppliers to actively invest resources to improve the safety and security of personal data.

Entering the Internet of Things era, our business has spread across five continents of the world. Even in countries with the strictest privacy protection laws and regulations, we have full confidence to meet and/or even exceed regulatory requirements. With the implementation of GDPR, Throughtek will continue to strengthen the security of personal data, personnel, equipment management and resource security to ensure the security of personal data, and continuously optimize user privacy management system to implement the protection of personal data.

3. Our Understanding of GDPR

3.1 GDPR consists of six core principles and derives the rights of the

individual and the corresponding security requirements:

- Legitimacy, Fairness and Transparency: Individual personal data must be processed in the manner prescribed by GDPR, and corporate information shall not be concealed from the individual. To ensure transparency, corporate organizations must clearly state in the privacy policy what types of data are collected and why.
- Restricted purpose: Personal information can only be collected for specific, clear and reasonable purposes.
- Minimum data collection principles: Personal data obtained in accordance with the purpose of collection must be within the scope of the appropriate, relevant, and necessary to achieve the purpose.
- Correctness: Personal data should be updated correctly and as needed. Individuals have the right to request correction or deletion of incomplete or incorrect funds.
- Shelf-life: All information of the individual can be identified and can only be retained within an appropriate period of time. Once the business organization exceeds the time frame, all information must be deleted.
- Integrity and confidentiality: The data collection process must comply with appropriate security standards, including measures to protect data from unauthorized or illegal interception, accidental loss, rewriting or damage.

3.2 The privacy protection requirements related to these principles include the following main points:

- Individuals have the right to know the purpose of collecting and processing personal data by government agencies, profit or

non-profit organizations. In addition, individuals have the right to delete or correct their data, request their data to no longer be processed, object to direct marketing, and withdraw their consent for the specific purpose of their data collected. The right to data portability gives individuals the right to move their data elsewhere and obtain relevant assistance in this regard.

- The organization must protect individual personal data in different ways depending on the sensitivity. If a leak occurs, the Data Controller must notify the appropriate authority/individual within 72 hours. In addition, if the leakage of the information results in a high degree of risk to the individuals' rights and freedoms, the organization must also notify the affected individuals.
- The processing of personal data must be based on law. Any consent to the processing of personal data must be "for free, specific, fully informed, and clear." Especially to protect children, GDPR has some additional consent requirements when dealing with underage individuals.
- When necessary, the organization must conduct data protection impact assessments to understand the privacy impact of the project or process and take necessary improvement measures. Concerns about handling activities, processing data, and other relevant records of the GDPR regulations must be properly preserved.

- GDPR compliance measures are not one-time procedures but rather activities that the organization should continue to perform. Non-compliance with GDPR regulations may result in large fines.

Note: The above regulatory requirements are only subjective interpretations of GDPR by ThroughTek and can be used as a reference for readers of this article. However, ThroughTek is not a legal office, so readers of this article should not use this as a substitute for legal advice. ThroughTek assumes no responsibility for any action taken based on part or this entire article.

4. Our Work on GDPR Compliance

4.1 Enhance privacy awareness and related educational training

As a basic work to strengthen the protection of personal data and complete GDPR compliance, we have selected senior management to receive relevant training from external professional organizations, and provided educational training for the entire company to ensure that everyone in the company has a basic understanding of GDPR concepts and requirements and further strengthening team privacy awareness:

- Two supervisors participated in the basic GDPR course organized by BSI

- Established an internal GDPR task force as a platform for information exchange and discussion

- Organize GDPR related information and open access for the entire company

- Explain the GDPR concept to all employees and the highest

management level through educational training courses

- Through remote web meetings and internal meetings to ensure that our partners and customers understand GDPR and their impact.

4.2 Understanding the Data We Have or Process

One of the key points of GDPR compliance preparation is to identify which types of data are personal owned or processed, and to clarify whether it contains the personal data under the definition of GDPR. Only by knowing what kind of resources and locations of data are collected, processed, or stored will it be possible to further construct appropriate personal data protection mechanisms, so we proceeded to:

- Inter-departmental discussions confirm data definition and data classification
- Global data consolidation within the company group
- Company website personal data collection (including cookies) and adjustment of consent method

4.3 Updating Company's Existing Policies and Operating Procedures

In order to achieve many of the personal data protection standards established by GDPR, not only our company, but the vast majority of multinational corporations must change existing management

systems and procedural approaches. ThroughTek will continuously adjusts existing work guidelines and processes to ensure the security, integrity and availability of data. When a notification of infringement incidents occurs, ThroughTek can then promptly notify the authorities and data owner within 72 hours in accordance with legal requirements:

- Integrate ISO 27001 / ISMS Information Security Management System
- Update data protection and company privacy policy
- Data Collection and Consent Usage Form / Content Adjustment
- Update data leak management procedure
- Develop emergency response procedures

4.4 Product and Services Protection Optimization and Contract Review

Integrate the principle of Privacy by Design into the process of product development and optimization, strengthen cross-border transmission of security and regulatory data, and cooperate with or actively review stake management processes with stakeholders. Based on situation, discuss the rights and obligations related to personal data protection and resources that are regulated by the contracts:

- Update service plans and products that enhance privacy protection for users in response to GDPR

- More secure encryption technology for data transmission

- Adjustment of the technical framework of the service to ensure that EU residents' personal data will not be transferred outside the EU

- Provide customers with information on handling and protective measures

- Review the contracts of users, business partners and suppliers

4.5 Appointing Data Protection Officer

The GDPR requires companies to establish a job titled "Data Protection Officer (DPO)" under certain conditions. To this end, ThroughTek officially appointed Frank Huang as Data Protection Officer on June 1, 2018, responsible for overseeing data protection policies and ensuring that all procedures meet the GDPR requirements.

5. Data Privacy Protection Technology Challenges

As part of strengthening the individual's degree of control over its own personal data, GDPR has proposed "Right to Data Portability", requiring the Data Controller to provide personal data to the individual in a

standard common format and if the individual requests to send data to a third party, including a competitor, the Data Controller must also provide support.

In general, switching between platforms is difficult. For example, the data structures used by most account login platforms cannot be used interchangeably. We are actively researching how to make our services and products data-portable. We are referencing and studying Alibaba and Carnegie Mellon University's privacy protection technologies research, and understanding the technical solution options and costs for data portability in cloud services.

6. Conclusion

Under the requirements of GDPR, how to allow individuals to exercise privacy-related rights has become one of the company's most important operational issues. For example, GDPR has increased the right to request the deletion of personal data, allowing individuals to request the Data Controller to delete all personal data, and in some cases requiring all other data resources and processors must comply with the request as well. The under-discussion data portability condition of GDPR also requires the Data Controller to provide personal data to the individual in a standard common format, and when the individual explicitly requests, the Data Controller must even transfer the personal data to a competitor.

When using Throughtek services, customers can be assured that our services are fully protected and compliant, but this is only for customers using Throughtek's services. Throughtek highly recommend customers engaged in personal data related services to thoroughly analyze their own overall personal data usage process and make appropriate

adjustments in order to execute GDPR requirements.
In short, Throughtek Technology meets the GDPR regulations, but does not necessarily mean that our customers fulfill GDPR regulations.

Throughtek not only fully complies with laws and regulations, but is also happy to assist customers in complying with the applicable GDPR specifications for their business activities, such as deleting, correcting, transmitting, accessing, and objecting to personal data processing, and to further develop technologies that meet customer needs. We are also willing to share our process of planning and implementation of GDPR and provide our experiences to our customers for reference.

TUTK

Pioneering M2M Solutions

www.throughtek.com

9F, No. 364, Sec. 1, Nangang Rd.,
Nangang Dist., Taipei City 11579,
Taiwan

+886-2-2653-5111