Making Personal Data Safer with GDPR

As the implementation date of the EU's General Data Protection Regulation (GDPR) draws nearer, thousands of companies will soon be required to comply with GDPR-mandated data management laws. In the face of compliance, the following questions about GDPR often arise:

- What is GDPR and what's its relationship with companies and individuals?
- How does GDPR protect personal data?

Dahua hereby provide a brief introduction to GDPR.

Background to GDPR Formulation

In 1995, the European Union introduced the Data Protection Directive ("Directive", hereafter) which established minimum standards for the legislation of personal data protection in EU member states. At that time, the scope of personal data collection processing was limited to usernames, addresses, and relatively simple financial information. However, in the over 20 years since then, leaps in technology have lead us to a new era of information networking featuring big data and cloud computing. Today, as people enjoy the convenience of online services, they are also increasingly concerned with the protection of the personal data they produce or provide. The EU has responded to these concerns with the General Data Protection Regulation (GDPR) on April 4th, 2016, after many years of legislation and negotiation. The GDPR implementation date has been set as May 25th, 2018, thus presenting a new challenge in the protection of personal data.

Applicable Scope of GDPR

You may be thinking that since the GDPR was created by the EU, it has nothing to do with companies located outside of the region. Unfortunately, that assumption is very wrong. The GDPR application scope not only encompasses companies operating within the EU, but also those located outside of the EU providing internet or business services to EU-based customers. In other words, no matter where a company is located, as long as it processes the personal data of customers located with the European Union during the provision of products or services, it must comply with GDPR.

GDPR Compliance Requirements for companies

How does the GDPR regulate the protection of personal data for companies providing internet and business services?

1. With regards to the processing of data, companies must comply with the following:
    a) Legality: All personal data used, processed, and transacted for business purposes must comply with legal requirements.
    b) Fairness: During the usage and processing of data, the interests of all subjects involved must be properly balanced. Sacrificing the interests of the Data Subject to for business use of personal data and for economic benefits is prohibited.
    c) Transparency: The objectives, scope, and mediums in which data is used and transacted should only be performed when the Data Subject has knowledge of these actions. It is prohibited to process or transact data without the Data Subject's knowledge.

In addition, GDPR has also stipulated "categorical constraints," "data minimization," "precision,"

“storage restrictions,” “completeness and secrecy,” and “accountability mechanism” principles.

2. Companies should establish a complete internal accountability system

Companies should set up a thorough institutional arrangement, including data safety management processes, leak discovery methods, data breach notification policies, etc., to satisfy strict requirements of the “Directive”.

a) Data Protection Officer (DPO): Companies must set up a Data Protection Officer to communicate with data protection supervision institution. The Data Protection Officer must report to the GDPR committee, and has the right to supervise company data processing.
b) Documented Management: Companies must completely record all data processing events, creating searchable records for each action. Documented management is not only an internal management procedure, but also the handle of the data protection institution to enforce these requirements.
c) Data protection impact assessment and prior consultation: In regards to high-risk data processing actions, companies must first perform a data protection impact assessment. If the results of this assessment indicate high risk, and the company involved has no mechanism of reducing risk, the company shall engage in prior consultation about the data processing activity with the data protection institution.
d) Event response: Companies must have a response plan in case of data breaches. As soon as a data breach occurs, the company must inform the data supervision institution within 72 hours.
e) Safety Assurance Measures: Companies must specifically take the below measures to ensure data safety:
    1. Anonymization and pseudonymization of personal data.
    2. Ensure long-term confidentiality, integrity, usability, and systematic recovery capabilities.
    3. Immediate data recoverability and accessibility of data in the event of physical or technological faults.
    4. Establish periodic testing, assessment, and evaluation of technology and management measures to determine system validity.

Personal Rights under GDPR Regulations

GDPR gives more comprehensive rights to individuals with respect to how their data is processed, allowing us to be in control of our personal data, and achieving better protection of personal data.

What kind of rights does GDPR grant to us?

GDPR grants the owners of individual data strong rights, enacting detailed regulations on Data Subjects’ right to know, right of access, right to object, right to data portability, and right to erasure:

- Right to Know: The Data Controller must inform individuals in a clear and concise manner how their data will be collected and processed.
- Right to access: The Data Controller must provide users with a process to access their data. If this request is electronic, the data must be provided to individuals electronically.

The Data Controller cannot charge for this service unless the Data Subject's request is excessive and surpasses the controller's burden.

- Right to object: Data Subjects have a permanent right to object to the Data Controller's right to process personal data, and have a permanent right to refuse marketing activities based on personal data. The "Directive" also introduce rights to restrict processing, such as when the Data Subject files a complaint (for example, against the accuracy of the data), the Data Subject has not demanded the deletion of data, but can limit the Data Controller from continuing to process the subject's data.
- Right to Data Portability: Individuals can seamlessly transfer their personal data and materials from one information service provider to another. This right means that the Data Subject possesses strong rights over the control and management of their personal data.
- Right to Data Erasure: Data Subjects have the right to demand the Data Controller that their data be erased and not spread. This purpose of introducing this right is to resolve privacy risks associated with the storage of high volumes of personal data, thus strengthening the personal privacy protections afforded to the Data Subject.

Severe GDPR Penalties

In addition to setting a series of unified laws and stricter regulations towards the processing of personal data, the GDPR has also set forth harsh penalties for violations. These penalties are in the form of administrative fines, and shall be enforced on those engaging activities violating GDPR. Depending on the degree of infraction, the highest penalties deal out fines on two levels:

1. 10 million Euros or 2% of annual global turnover
2. 20 million Euros or 4% of annual global turnover

Severe penalties force corporations to pay attention to their GDPR compliance. The key factor in avoiding penalties is refraining from data breaches and proper control over data processing procedures.

Dahua and GDPR Compliance

Dahua Technology, a leading solution provider in the global video surveillance industry, has always been committed to the protection of personal privacy and data security.

Following the arrival of GDPR, and as video recording includes personal data, Dahua is further increasing its emphasis on personal data protection. Dahua products are designed to satisfy the legality, fairness, and transparency of personal data processing. They also provide comprehensive data protection measures, encrypting personal data and engaging in anonymization and pseudonymization. In regards to management systems, Dahua will continue to improve its data protection process via the establishment of more complete internal management processes and the enhancement of accountability.

The use of Dahua products will assist you in better complying with GDPR. We will continue to develop more features which allow the implementation of higher safety security solution with better personal privacy protection.