EU GENERAL DATA PROTECTION REGULATION

GENERAL INFORMATION DOCUMENT

This resource aims to provide a general factsheet to Asia Pacific Privacy Authorities (APPA) members, in order to understand the basic requirements included in the EU General Data Protection Regulation (GDPR). APPA members can then use this document to develop their own guidance to assist their businesses and other organizations processing the personal data of European individuals in complying with the GDPR.

ARTICLE 29
Data Protection Working Party

Key Facts

The GDPR becomes applicable from **25 May 2018** in all member states of the European Union (EU) and contains a full set of requirements building on existing principles and introducing some new concepts.

- The GDPR is directly applicable at national level and **harmonizes data protection laws across the EU**. It replaces the current 1995 Data Protection Directive (Directive 95/46/EC). However, in certain limited occasions, the GDPR leaves some flexibility to Member States for national transposition, as such Member States have to introduce national provisions to complement the GDPR.

- The GDPR applies **to data controllers and data processors established in the EU.** It also becomes applicable to data controllers **or processors offering goods or services to the EU** or monitoring the behavior of individuals in the EU**.**

- The GDPR does not apply to certain processings covered by the Law Enforcement Directive (Directive 2016/680/EC), processing for national security purposes and processing carried out by individuals purely for personal/household activities.

12 Key Messages

1. Material Scope of the GDPR – (Article 2)

The GDPR applies to the processing of personal data. Personal data is defined as any information relating to an identified or identifiable natural person and includes data such as an IP address, an email address or a telephone number. Processing activities include, among others, the collection, use and disclosure of the data.

The GDPR provides for additional protection to the processing of special categories of personal data. Such special categories include, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and genetic and biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Member States may introduce further conditions, including limitations, with regard to the processing of genetic and biometric data or data concerning health.

2. Territorial Scope of the GDPR – (Article 3)

The GDPR applies to data controllers and data processors with an establishment in the EU, **or** with an establishment outside the EU that target individuals in the EU by offering goods and services (irrespective of whether a payment is required) or that monitor the behavior of individuals in the EU (where that behavior takes place in the EU). Factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

Data controllers and/or data processors not established in the EU, but whose activities fall within the scope of the GDPR, will generally (some exceptions apply) have to **appoint a representative established in an EU member state**. The representative is the point of contact for all Data Protection Authorities (DPAs) and individuals in the EU on all issues related to data processing (Article 27).

> *Example: A Japanese web shop, offering products, available online in English with payments to be made in Euros, processing multiple orders a day from individuals within the EU and shipping these products to them, should be compliant with the GDPR*

3. Fundamental principles relating to processing – (Article 5)

According to the GDPR, personal data must be processed in accordance with the **principles of lawfulness, fairness and transparency**. In addition such data must be collected for specified, explicit and legitimate purposes and not further processed in an incompatible manner to those purposes (**principle of purpose limitation**). A data controller or a data processor must also make sure to respect the **principle of data minimization**, meaning that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they were processed. Personal data must be **accurate** and, where necessary, kept up to date. In addition, the **accountability** principle is recognized itself as a fundamental principle. Finally, the **principles of storage limitation** and **integrity and confidentiality** have to be respected. Therefore, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are

processed and must be processed in a manner that ensures appropriate security of the personal data.

4. Lawfulness of processing – (Article 6)

Under the GDPR, a processing of personal data will only be lawful if, at least one of the conditions below is met:

- the data subject has provided **consent** to the processing,
- the processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- the processing is necessary for **compliance with a legal obligation** to which the controller is subject,
- the processing is necessary to **protect the vital interests** of the data subject or of another natural person, or
- the processing is necessary for the **performance of a task carried out in the public interest**
- the processing is necessary for the purposes of the **legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Specific and stricter requirements are defined concerning the processing of **special categories of data** (article 9).

5. Consent – (Articles 4, 7 and 8)

The GDPR devotes several articles to clarify the notion of consent.

Under the GDPR, which reflects the WP29's opinion on consent requirements[1], **consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes** which by a statement or by a clear affirmative action, signifies agreement to processing.

The request for consent must be presented in a manner clearly distinguishable from other matters in an intelligible and easily accessible form, using clear and plain language. The data subject must be able to easily withdraw his or her consent at any time and must be informed of this right in advance.

Specific requirements apply in relation to children's consent for information society services. If an individual below 16 years wishes to use information society services, consent must be obtained from the child's parent or the holder of parental responsibility of the child in question. However, Member States may introduce domestic laws to lower this age to not less than 13 years.

6. Individual Rights – (Articles 12 – 23)

The GDPR **maintains, often reinforces and further develops the rights of the individuals** (information, access, rectification, objection, erasure restriction right to be forgotten right to data portability.

- The **right to information** requires data controllers to give individuals certain information about the processing of their personal data free of charge (exceptions apply – Article 14). This information must be provided in a concise, transparent,

[1] Opinion 15/2011 on the definition of consent, 13 July 2011, WP187

intelligible and easily accessible form using clear and plain language. Data controllers can provide such information to individuals in combination with standardized icons to give an easily visible, meaningful overview of the processing.

- **The right to be forgotten**, also referred as the right to erasure as it includes both the right to have the data erased and the right to delisting in certain circumstances. The individuals have the right to require data controllers to delete their data in certain circumstances, including where the information is no longer necessary for the purpose for which it was collected or where the individual withdraws their consent and there is no other legal grounds for processing their data.

- The **right to restriction of processing** applies in some specific circumstances including for example, for an interim period allowing the data controller to verify the accuracy of the personal data that is contested by the data subject, or when the controller no longer needs the personal data for the purposes of the processing but are required by the data subject for, for example, the establishment of legal claims.

- The **right to data portability** refers to the right of an individual to receive personal data that he/she has provided to the data controller in a structured, commonly used and machine readable format and to transmit that data to another data controller without hindrance. This right only applies to personal data that an individual has provided to the controller, where the processing is based on the individual's consent or for the performance of a contract and where the processing is carried out by automated means. The exercise of this new right to data portability shall be without prejudice to the exercise of the right to erasure or the right of access.

There are restrictions to these rights under Article 23 of the GDPR such as for example when this is necessary to safeguard national security, defense or public security in a democratic society.

7. Accountability obligations of data controllers– (Articles 5, 25, 30, 35 – 43)

According to the accountability principle (Article 5(2)), data controllers (i.e. the entities that define the purposes and means of the processing) have **to ensure compliance with the GDPR and be able to demonstrate such compliance**. The data controllers generally must implement appropriate technical and organizational measures, including data protection policies. In assessing which or how such measures should be implemented, the data controllers should consider the nature, scope, context and purposes of the processing as well as the risks for the rights and freedoms of individuals.

The GDPR provides data controllers with a complete set of tools to help demonstrate accountability, some of each have to be mandatorily put in place. For example, the establishment of a data protection officer (DPO) or conducting data protection impact assessments (DPIA), and the respect of the principles of privacy by design and privacy by default are mandatory. Data controllers can choose to use others such as the codes of conduct and certification mechanisms to demonstrate compliance with the principle of accountability.

For more information on the specific tools, please refer to the specific WP29 guidelines that can be found on the WP29 newsroom[2].

[2] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

8. Obligations of data processors – (Article 28)

The GDPR **introduces new requirements which apply directly to data processors giving them as such a separate legal status from that of the data controllers particularly with regards to security measures and international data transfers**.

Data processors, must provide the expected guarantees just as data controllers do and must also implement appropriate technical and organizational measures to ensure that the processing will meet the requirements of the GDPR. Data processors must also assist data controllers in matters of security, DPIA and data breach notifications and alert the controller if their processing instructions would lead to a possible violation of the GDPR or of a provision of Union or Member State law.

Processing by a processor shall be governed by a contract or other valid legal act that is binding on the processor by the controller. Besides the basic information required in this contract or other legal act such as the duration of the contract, the GDPR enumerates specific clauses that must be included, such as, for instance, that the data processor may only process data in accordance with documented instructions from the controller or that the processor cannot engage another processor without the authorization of the data controller.

9. Data breach notifications – (Articles 33 and 34)

Under the GDPR **data breach notifications to the Data protection Authority (DPA) are mandatory** unless such data breach is unlikely to impact the rights and freedoms of individuals. Data controllers must provide such notification to the DPA without undue delay and, where feasible, **not later than 72 hours after having become aware of it.**

In some cases – when the breach is likely to result in a high risk to the rights and freedoms of natural persons – such notification must also be made to the relevant data subjects without undue delay.

The data processors must notify the data controller of the data breach without undue delay.

10. International Transfers – (Articles 44 – 49)

Under the GDPR, **personal data may be transferred outside the EU to third countries or international organizations that provide an "adequate level of data protection", meaning "essentially equivalent" to the level of protection afforded within the EU.**

A transfer of personal data to a third country or international organization that is not afforded a European Commission decision of adequacy can be made where appropriate specific safeguards are in place. Such safeguards can be brought through a number of available tools such as standard data protection clauses, binding corporate rules, and by new tools -approved codes of conduct or certification.

Where there is no adequacy decision and no appropriate safeguards in place a transfer of personal data can only be made in limited situations for example, where an individual explicitly consents to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer or if the transfer is necessary for the purposes of compelling legitimate interests.

Onwards transfers to other third countries are also covered by these requirements.

Example: A subsidiary company in the European Union uses a centralized human resources system in India belonging to its parent company to store information about its employees. Appropriate safeguards need to be put in place to frame the transfers of data from the European Union based subsidiary to the parent company in India.

11. Supervision, Cooperation, Remedies – (Articles 50 and 83)

In general, GDPR reinforces the independence requirements and the role of DPAs. They benefit from a wide range of consultative, investigation and corrective powers, among which the one to impose administrative fines.

The GDPR significantly toughens the approach to and the level of administrative fines foreseen in the EU and harmonizes it.

DPAs will have the power to impose administrative **fines reaching up to 20 million euros or 4% of the annual worldwide turnover** for certain infringements of the GDPR provisions.

The GDPR also introduces a new procedure for **collective actions before the DPAs** within the EU, and provides for the possibility to foresee a similar procedure before the courts of Member States wishing to introduce collective actions at the national level.

The GDPR also encourages the EU Commission and DPAs to cooperate for its effective application. The WP29 members are looking at possible options to develop this cooperation and will discuss ideas with their APPA counterparts when they have finalized these ideas, in order to remain open to proposals from APPA members.

12. European Data Protection Board (EDPB) – (Articles 64, 65, 66 and 68)

The Article 29 Working Party (WP29), set up under Directive 95/46/EC, is composed of the EU's national supervisory authorities, the European Data Protection Supervisor ("EDPS") and the European Commission. The WP29 will be replaced by the "European Data Protection Board" ("EDPB").

The EDPB is given a long and detailed list of tasks, but its primary role will be to contribute to the **consistent application of the GDPR** throughout the Union. The EDPB will have the status of an EU body with **legal personality and extensive powers** to settle disputes between national supervisory authorities and issue opinions on specific matters such as list of risky processing, codes of conduct and certification bodies' accreditation criteria. The EDPB will also be responsible for issuing guidelines, recommendations and best practices.

The EDPB will be represented by its Chair. The EDPB will also have a Secretariat which will assist the Chair and the Board in their tasks.

13. One Stop Shop

The GDPR provides new methods of co-operation and consistency through for example, the "*one stop shop*" mechanism, for entities having cross-border processing in multiple EU countries.

A cross-border processing exists when either controllers or processors carry out activities through establishments in multiple Member States or where there is a single establishment but with processing activities that substantially affect or are substantially likely to affect data subjects in multiple Member States.

Put simply, a 'lead supervisory authority' is the contact point of the controller/processor in relation with the given cross-border processing and has the primary responsibility for dealing with such cases, for example the lead supervisory authority will coordinate any investigation related to the cross-border processing, involving other 'concerned' supervisory authorities.

However, each DPA will be competent to handle local complaints or infringements of the GDPR.

It is important to note that the GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the European Union. If the company does not have an establishment in the EU, the mere presence of a representative in a Member State does not trigger the one-stop-shop system. This means that controllers without any establishment in the EU must deal with supervisory authorities in every Member State they are active in, through their local representative.

For more information on the lead supervisory authority please see the relevant WP29 guidelines[3].

[3] Guidelines for identifying a controller or processor's lead supervisory authority, 13 December 2016, WP244