THE GENERAL DATA PROTECTION REGULATION: GDPR

Dr. Sitdhinai Chantranon
Director, Office of Executive Vice President
Legal and General Administration
Thai Airways International PCL

SCOPE OF APPLICATION

- Article 2 1) This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

- Article 3 1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

- Article 3 2) extend territorial scope (Extraterritorial scope) applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

EXCEPTION OF SCOPE OF APPLICATION

Article 2(2) This Regulation does not apply to the processing of personal data:

- (a) in the course of an activity which falls outside the scope of Union law;
- (b) by a natural person in the course of a purely personal or household activity;
- (c) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

DEFINITIONS OF DATA CONTROLLER, DATA PROCESSOR AND PROCESSING

- ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

DEFINITIONS OF PERSONAL DATA AND SENSITIVE PERSONAL DATA

- **'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an**

- **identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;**

- **Sensitive personal data e.g.** Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Genetic data, Biometric data, Health , Sex life or sexual orientation

PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

1) Lawfulness, fairness, and transparency principle
2) Purpose limitation principle
3) Data minimization principle
4) Accuracy principle
5) Storage limitation principle
6) Integrity and confidentiality principle
7) Accountability principle

LAWFULNESS FOR PROCESSING OF PERSONAL DATA

- Processing shall be lawful only if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

- Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

LAWFULNESS FOR PROCESSING OF PERSONAL DATA(CONT.)

Except from the consent, the processing shall be lawful for any of the following conditions

- (1) 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;
- (2) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (3) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (4) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (5) 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.

PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

Processing of personal data revealing special categories shall be prohibited, except;

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified Purposes;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA (CONT.)

- (f) processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

- (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

- (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards

- (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

CONDITIONS APPLICABLE TO CHILD'S CONSENT

- in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
- Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13

  years.

RESPONSIBILITY OF THE CONTROLLER

- The Controller has obligation to use security measures to protect personal data as follows:
- 1) The controller and the processor shall designate a data protection officer in any case where:
- (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale ;or
- (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences
- 2) implement appropriate technical and organisational measures for ensuring that processing is performed in accordance with the GDPR
- 3) carry out an assessment of the impact of the envisaged processing operation on the protection of personal data where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons
- 4) designate a representative in EU in case a processor is not established in the EU
- 5) keep the record of processing
- 6) notifying the breach to the Supervisory Authority

RESPONSIBILITY OF PROCESSOR

- 1) designate a data protection officer , if necessary
- 2) keep the record of processing
- 3) implement appropriate technical and organisational measures for ensuring that processing is performed in accordance with the GDPR
- 4) designate a representative in EU in case a processor is not established in the EU
- 5) cooperation with the Supervisory Authority
- 6) notifying the breach to the controller without delay
- 7) comply with conditions for transfer of data to third country or international organisations.

RIGHTS OF DATA SUBJECT

- 1)Right to be informed of information when personal data are obtained from the data subject
- 2)Right to be informed of information when personal data are not obtained from the data subject
- 3) Right of access by the data subject
- 4) Right to rectification
- 5) Right to erasure (‘right to be forgotten’)
- 6) Right to restriction of processing
- 7) Right to data portability
- 8) Right to object
- 9) right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects

NOTIFICATION OF A PERSONAL DATA BREACH TO THE SUPERVISORY AUTHORITY

- In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

  - Confidentiality Breach
  - Integrity Breach
  - Availability Breach

- When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay

- unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, or the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption,

- or the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise,

- or it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner

SUPERVISORY AUTHORITY

- Each Member state shall provide one or more independent public authorities (Supervisory authority) for monitoring the application of GDPR

PENALTY

- Administrative fines up to 20 M EUR or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

- The Regulation provides for the transfers of personal data to third countries in 3 scenarios ;

- 1)Transfers on the basis of an adequacy decision(Adequate level of protection) e.g. List of adequate countries or where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

- 2) Transfers subject to appropriate safeguards e.g.
  - a legally binding and enforceable instrument between public authorities or bodies;
  - Binding Corporate Rules
  - standard data protection clauses adopted by the Commission in accordance with the examination procedure3)
  - standard data protection clauses adopted by a supervisory authority and approved by the Commission
  - an approved code of conduct
  - an approved certification mechanism

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS (CONT.)

- 3) Derogations for specific situations
- (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

  (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of public interest;
- (e) the transfer is necessary for the establishment, exercise or defense of legal claims;
- (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

PERSONAL DATA COLLECTED BEFORE THE EFFECTIVE DATE

- The Regulation does not provide the provisional clause, hence applies immediately on the effective date, i.e.
- 25 May 2018.
- Previous consent given does not valid.