Tilleke & Gibbins

bangkok | hanoi | ho chi minh city | jakarta | phnom penh | vientiane | yangon

Legal Developments in Data Privacy

David Duncan

23 May 2018

Data Privacy Developments

- GDPR (Europe)
- Personal Data Protection Bill (Thailand)

GDPR

- General Data Protection Regulation
- 2016/679
- Adopted on 14 April 2016
- Becomes effective 25 May 2018
- Directly applicable; member states need not enact implementing legislation

GDPR: Territorial Scope

- 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.
- This Regulation 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:
  - 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
  - the monitoring of their behaviour as far as their behaviour takes place within the Union.
- This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

"Processing"

- '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

Controller vs. Processor

- '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

Controller

- Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
  - the pseudonymisation and encryption of personal data;
  - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Processor

- Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
- The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
- Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:
  - processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
  - ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
  - takes all measures required pursuant to Article 32;
  - respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;
  - taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;
  - assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;
  - at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
  - makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
- With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

Data Protection By Design and By Default

- Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
- The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
- An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Data Protection Impact Assessments

- Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
- The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
- A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
  - a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
  - processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
  - a systematic monitoring of a publicly accessible area on a large scale.
- The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Key Requirements

- Lawful basis for processing
- Sensitive data
- Transfer restrictions
- Handling data breaches
- Record keeping
- Rights of data subjects
- Data Protection Officer

Lawful Basis for Processing

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- 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;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 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;
- 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.

Consent

- Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
- The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Sensitive Data

- Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, 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 shall be prohibited.
- Unless…

Sensitive Data

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- 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;
- 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;
- 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;
- processing relates to personal data which are manifestly made public by the data subject

Sensitive Data

- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- 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;
- 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 referred to in paragraph 3;
- 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;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on 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.

Transferring Data Abroad

- Transfers on the basis of an adequacy decision
- Transfers subject to appropriate safeguards
- Binding corporate rules
- judgment of a court or tribunal and any decision of an administrative authority of a third country, based on international agreement
- Others

Transfers Subject to Appropriate Safeguards

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with Article 47;
- standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
- standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
- an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

(authorization from supervisory authority not needed)

Transfers Subject to Appropriate Safeguards

- contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

(also requires authorisation from supervisory authority)

Others

- 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;
- 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;
- 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;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- 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;
- 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.
- only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data (requires notice to supervisory authority and must inform the data subject).

Data Breaches

- 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 in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
- The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
- The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Data Breaches

- 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 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;
  - the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
  - 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.

Record Keeping

- Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
  - the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
  - the purposes of the processing;
  - a description of the categories of data subjects and of the categories of personal data;
  - the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
  - where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
  - where possible, the envisaged time limits for erasure of the different categories of data;
  - where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Record Keeping

- Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
  - the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
  - the categories of processing carried out on behalf of each controller;
  - where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
  - where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Data Protection Officer

- The controller and the processor shall designate a data protection officer in any case where:
  - the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
  - 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
  - the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

Rights of Data Subjects

- Informational rights
- Access rights
- Right to rectification
- Right to erasure
- Right to object to processing
- Right to restriction of processing
- Right to data portability
- Right not to be subject to a decision based solely on automated processing which produces legal effects concerning him or her or similarly significantly affects him or her

Informational Rights (Collection from Data Subject)

- Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
  - the identity and the contact details of the controller and, where applicable, of the controller's representative;
  - the contact details of the data protection officer, where applicable;
  - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
  - where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
  - the recipients or categories of recipients of the personal data, if any;
  - where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
- In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
  - the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
  - the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
  - where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
  - the right to lodge a complaint with a supervisory authority;
  - whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
  - the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Informational Rights (Not Collected from Data Subject)

- Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
  - the identity and the contact details of the controller and, where applicable, of the controller's representative;
  - the contact details of the data protection officer, where applicable;
  - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipients of the personal data, if any;
  - where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.
- In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:
  - the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
  - where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
  - the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
  - where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
  - the right to lodge a complaint with a supervisory authority;
  - from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
  - the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- The controller shall provide the information referred to in paragraphs 1 and 2:
  - within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
  - if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
  - if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Right of Access

- The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
  - the purposes of the processing;
  - the categories of personal data concerned;
  - the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
  - where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
  - the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
  - the right to lodge a complaint with a supervisory authority;
  - where the personal data are not collected from the data subject, any available information as to their source;
  - the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
- The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Right to Rectification

- The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to Erasure

- The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
  - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
  - the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
  - the personal data have been unlawfully processed;
  - the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
  - the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
- Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
- Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
  - for exercising the right of freedom of expression and information;
  - for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
  - for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
  - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
  - for the establishment, exercise or defence of legal claims.

Right to Object to Processing

- The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
- Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
- At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
- In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
- Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Right to Restriction of Processing

- The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
  - the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
  - the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
  - the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
  - the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
- Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
- A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Right to Data Portability

- The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
  - the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
  - the processing is carried out by automated means.
- In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

Right Against Automated Processing

- The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
- Paragraph 1 shall not apply if the decision:
  - is necessary for entering into, or performance of, a contract between the data subject and a data controller;
  - is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
  - is based on the data subject's explicit consent.
- In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
- Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(2)1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Remedies and Penalties

- Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
- Administrative Fines
  - Up to EUR 10 million or 2% of total annual worldwide turnover for the previous financial year (whichever is higher)
  - Up to EUR 20 million or 4% of total annual worldwide turnover for the previous financial year (whichever is higher)

Data Privacy Law in Thailand

- Provisions of/Regulations issued under:
  - Credit Information Business Act
  - National Health Act
  - Telecommunications Business Act
  - Frequency Allocation Act
  - Financial Institutions Business Act
  - Payment Systems Act
  - Etc.

Personal Data Protection Bill

- Pending since early 2000s
- Similar coverage to GDPR, though Personal Data Protection Bill is less detailed (many parts contemplate regulations to be issued)

Personal Data Protection Bill

- The personal data controller may not collect, use, or disclose personal data if the owner of the personal data has not given consent at or before that time, unless otherwise provided by this Act or other law.
- The personal data controller may not collect personal data without the consent of the owner of the personal data, unless
  - for the benefit of study, research or statistics, and keeping personal data for that purpose confidential;
  - to prevent injury to the life or health of a person;
  - data disclosed to the public with explicit or implied consent of the owner of the personal data;
  - It is necessary for the performance of a contract to which the owner of the personal data is party or for use in proceeding with the request of the owner of the personal data before entering into a contract;
  - It is necessary for public interest;
  - It is necessary for the legitimate interests of the personal data controller, or that of a person or entity other than the personal data controller, except where such interests are less important than the basic rights of the owner in the personal data;
  - It is lawful or according to an obligation of the personal data controller; or
  - Other cases as prescribed in Ministerial Regulations.

Consent

- Requests for consent must be made in writing, which may be done electronically.
- The personal data controller must specify the purpose of the collection, use, or disclosure.
- Consent must not be fraudulent or illegal, or based on a misunderstanding of the owner of the personal data as to the purpose.
- The Commission will specify a form for the consent.
- The owner of the personal data can withdraw consent at any time, unless there is a restriction on withdrawing consent by law or a contract that is contrary to the owner of the personal data withdrawing consent.
- The personal data controller must inform the owner of the personal data of the effect of withdrawing consent.

Sensitive Data

- Without the consent of the personal data owner, prohibits the collection of personal information about ethnicity, political opinion, creed, religion or philosophy, sexual behavior, crime records, health information, or any other information that affects public feelings as determined by the Commission, except as provided in Section 21 (2) or (7), or as prescribed in Ministerial Regulations.

Transfer Restrictions

- Where a personal data controller transmits or transfers personal data to a foreign country, the receiving country must have standards of privacy protection to conform to the criteria for the protection of personal data as the prescribed by the Commission under Section 14 (5), except:
  - In compliance with the law;
  - With the consent of the owner of the personal data;
  - It is pursuant to a contract between the owner of the personal data and the controller of the personal data;
  - It is for the benefit of the owner of the personal data but the owner's agreement cannot be captured at that time; or
  - Other cases as prescribed in Ministerial Regulations.

Security

- The controller of personal data shall have the following duties:
  - Assess the impact on privacy of personal information on a regular basis, continually;
  - Provide appropriate security measures to prevent wrongful loss, access, modification, or disclosure of personal data;
  - If personal data is to be provided to a person or entity other than the personal data controller, the personal data controller must take action to prevent such person from using or disclosing personal data wrongfully;
  - Delete personal data when the retention period expires or such data is no longer needed or is excessive, in light of the purpose of collecting such personal data, or when the owner of the personal data has withdrawn consent, except for preservation purposes; and
  - Notify the owner of the personal data without delay, if a personal data breach exceeds the number of persons declared by the Commission, and act in conformity with the privacy notice and remedial measures prescribed by the Commission without delay.

Security

- The personal data processor has the following responsibilities:
  - Handle collection, use, or disclosure of personally identifiable information obtained from the personal data controller only, unless contrary to the law or provisions for protection of personal data under this Act;
  - Provide appropriate security measures to prevent wrongful loss, access, modification, or disclosure of personal information, and inform the personal data controller about possible personal data breaches; and
  - Prepare and maintain records of data processing activities according to rules and procedures prescribed by the Commission.

Records

- The personal data controller must record the following items as relevant to each owner of personal data:
  - Personal data collected;
  - Purpose of collecting personal data of each type;
  - Information about the personal data controller;
  - Personal data retention period;
  - Rights to access personal information, including conditions for the exercise of such rights;
  - Use and disclosure under Section 24 paragraph three; and
  - Denial under Section 26 paragraph three and Section 28 paragraph two.

Rights of Data Subjects

- Informational rights
- Right to access
- Right to correction
- Right to have information erased, use suspended, or anonymized

Remedies and Penalties

- A personal data controller causing damage to the personal data owner must pay compensation to the personal data owner, whether such arises due to intention, negligence, or carelessness of the personal data controller, unless the personal data controller proves that:
  - Such damage was caused by force majeure, or by act or omission of the owner of the personal data;
  - Such is due to an order of officials acting in their capacity as authorized in law; or
  - Such is fully compliant with the applicable privacy regulations.
- For substantive breaches, penalties include imprisonment up to six months and/or a fine of up to THB 500,000.

Contact Information

- David Duncan
- +66.2.056.5555
- david.d@tilleke.com
- www.tilleke.com