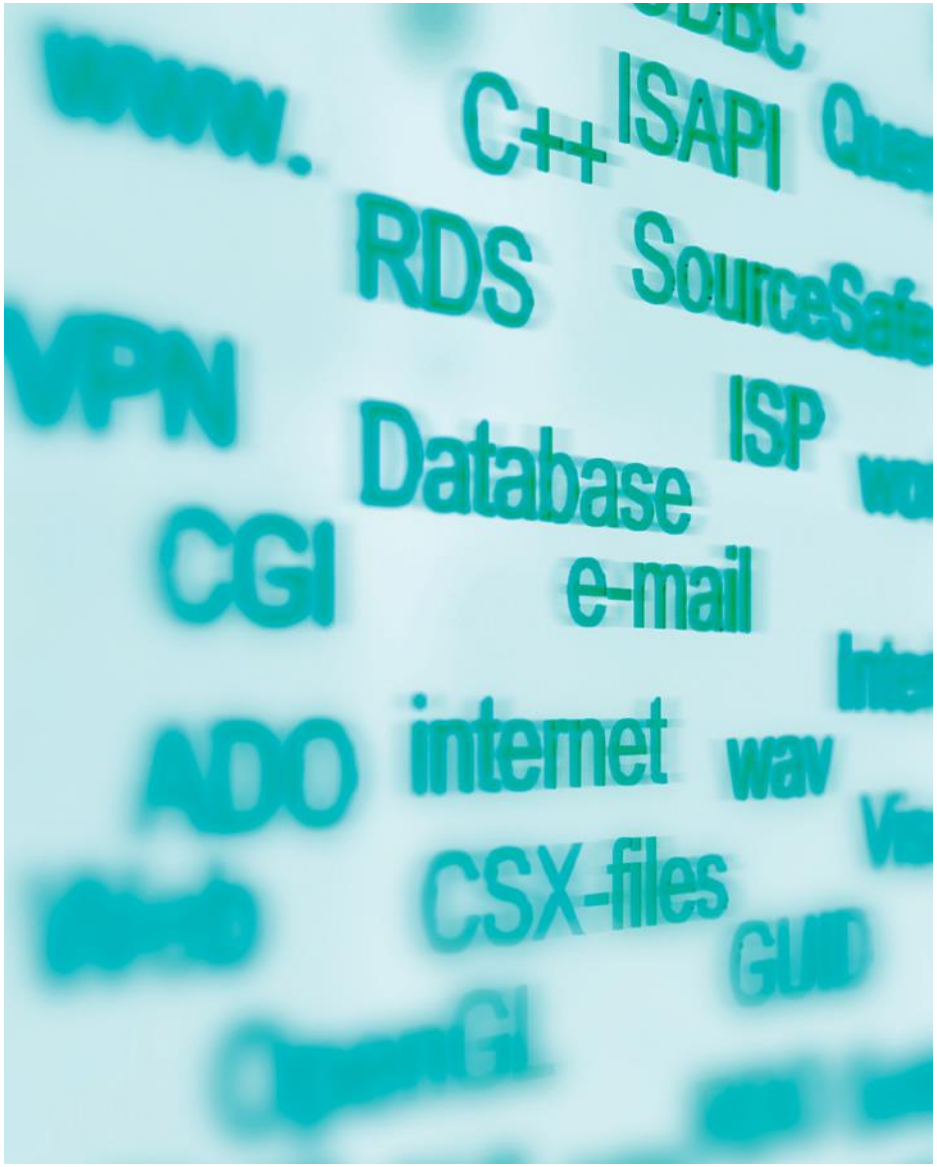
TaylorWessing

Prague

GDPR



Karin Pomaizlová, Taylor Wessing

19 September 2017

Contents

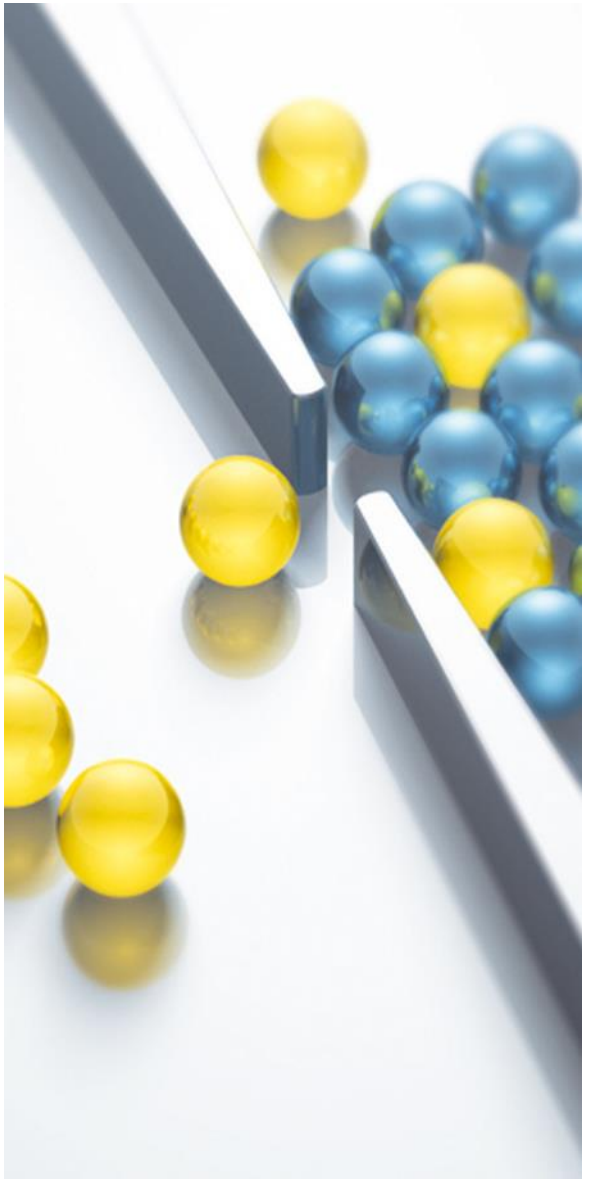
Legality of Data Processing – Article 6 GDPR

Processing shall be lawful only if and to the extent that at least one of the following applies:

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

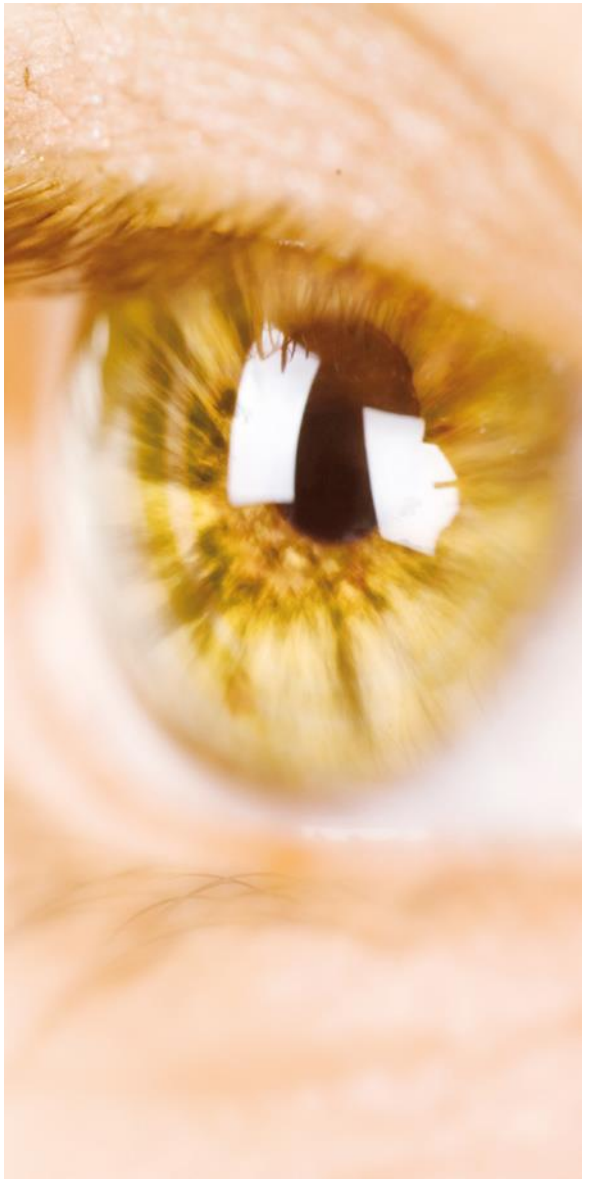
Consent

- Only one of legitimate grounds for data processing;
- Not a “silver bullet“;
- Data processing must be necessary and balanced;
- During data processing, it is always necessary to protect individuals from inappropriate interference with their privacy.
- Data processing is legitimate only if the purpose of processing cannot be achieved by other means.
- Data subject can withdraw his/her consent any time. It shall be as easy to withdraw as to give consent.



Definition of Consent

‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.



Consent Parameters

Consent freely given: Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. Therefore from the logic of it, consent shall be rarely applied in relationship between employers and employees.

Unconditional: Provision of services or delivery of goods should not be conditional to providing the consent.

Based on activity of data subject: In electronic communication there shall be no “pre-filled” tick boxes. In principal always “opt-in”.

Separation: The consent should be always separated from other contractual provisions, e.g. T&C, granting consent to send newsletters by e-mail.

Specific and unambiguous consent

> The purposes for which the personal data are processes need to be outlined specifically, unambiguously and they must be legitimate. It is necessary to set them out at the time of the collection of personal data.

"XXX uses the information we collect for XXX business purposes such as:

To provide the products and services you request.

To tell you about XXX products and services and those offered by our carefully selected business partners.

To manage our sites and services."

> The data subject should be informed of the existence of profiling and the consequences of such profiling for the data subject.

> When data are collected directly from the data subjects, controller should inform data subject, whether provision of the data is compulsory and consequences of failure to do so.

Information provided when asking for consent - I

Information to be provided where personal data are collected from the data subject:

> 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 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.

Information provided when asking for consent - II

To ensure fair and transparent processing the following information shall be also provided:

> 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;

> The right to lodge a complaint with a supervisory authority;

> The existence of automated decision-making, including profiling, as well as the significance and the envisaged consequences of such processing for the data subject.

Purpose of personal data processing

Even when granting consent to the processing of personal data, the specific purposes for which personal data is processed must be unambiguous and legitimate.

Personal data should be proportionate, relevant and limited to what is necessary for the purposes for which they are processed.

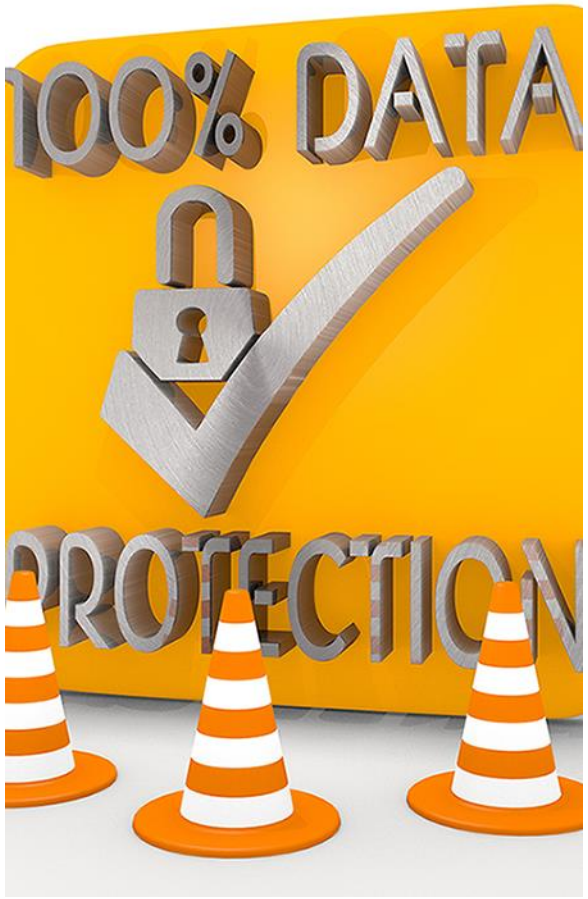
Consent from a child

- New conditions;
- 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 authorized 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
  [this will lead to partition of the unified conditions];
- The controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.

Processing of special categories of personal data

> The data subject has given explicit consent to the processing of those personal data for one or more specified purposes;

> Member States can provide that the prohibition to process special categories of personal data may not be lifted even by the data subject explicit consent;



Validity of consents granted prior to GDPR

Recital 171

…“Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force.

Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation.”

*In force as of 4 May 2018 (applicable as of 25 May 2018)

Data Protection Officer

The controller and the processor shall designate a data protection officer in any case where the core activities of the controller or the processor consist of processing personal data on a large scale that:

> Require regular and systematic monitoring of data subjects; or

> Concern special categories of data and personal data relating to criminal convictions and offences.

OR when required by national law [*this will lead to partition of the unified conditions*].

- A group of undertakings may appoint a single DPO provided that a data protection officer is easily accessible from each establishment.
- He/she can either be an outside contractor or an employee.
- The controller and the processor shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- The DPO shall directly report to the highest management level of the controller or the processor.
- The controller and processor shall support the data protection officer in performing his tasks besides other by providing resources necessary to carry out those tasks.

DPO tasks

The data protection officer shall have at least the following tasks:

- To inform and advise the controller or the processor and their employees;
- To monitor compliance with GDPR;
- Training of controller/processor employees;
- To provide advice where requested;
- Assist in impact assessment (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);
- To cooperate with the supervisory authority and contact point.

DPO and other positions within the firm

- Obligatory DPO and voluntary DPO;
- Voluntary DPO or „data manager“;
- Each manager shall assume responsibilities for protection of data within his area (finance, HR, sales, marketing);
- IT – who controls IT? Security.

Audit

- Due diligence across the firm based on top management initiative
- What personal data, in which form, for what purpose, from which source
- Archiving and liquidation data plan
- Legitimate basis for data processing
- Safety measures
- External processors
- Access rights
- Data transfer
- External audit - objective

Assessment of GDPR compliance

- Documentation
  (privacy policies, consents, contracts, information to data subjects)
- Data Breach scenarios
- Internal Standard Operation Procedures
- Costs for adoption of necessary measures
  v. Risks of penalties

Taylor Wessing Tools

www.taylorwessing.com/global-data-protection-guide

https://united-kingdom.taylorwessing.com/globaldatahub/article-gdpr-audit-checklist.html

https://france.taylorwessing.com/en/gdpr-assessment-tool

https://united-kingdom.taylorwessing.com/globaldatahub/article-privacy-policy-checklist.html

https://united-kingdom.taylorwessing.com/globaldatahub/article-breach-response-checklist.html

https://united-kingdom.taylorwessing.com/globaldatahub/article-data-controller-requirements-under-gdpr.html

https://united-kingdom.taylorwessing.com/globaldatahub/article-data-retention-policy-checklist.html

https://itunes.apple.com/gb/app/tw-cyber-response/id1230002282?mt=8
https://play.google.com/store/apps/details?id=com.taylorwessing.databreach&hl=en

Thank you for your attention!

Mgr. Karin Pomaizlová
Partner, Prague
Taylor Wessing CEE
k.pomaizlova@taylorwessing.com