Certain aspects of the controllers and processors obligations under GDPR from the challenge for the lawyer point of view.

(I) Main issue: The presentation covers kind of a road map of the new/modified obligations and shows two chosen important institutions in more details – **namely expended territorial reach of the GDPR and changes in contracting to process personal data**.

(II) Additional aspects: comments concernig the legal issues of which lawyers should be particulary aware of working with the text and with the specific stucture of the new Regulation, which may help to capture and analyse the controllers' and processors' new obligations properly and then give an appropriate expert advise to Clients.

Introduction

From the perspective of the theme of the conference - How the lawyers should be prepared –it is worth underlining that thinking of the new data protection provisions lawyers should have in mind all configurations of their possible legal interventions.

- so first of all we can provide a legal support to a controller or a processor from EU country, but also from outside of the EU,

- we are also controllers in our own legal businesses however this presentation focuses rather on general perspective of controllers and processors' obligations not on controller who is a lawyer,

- we can also represent data subjects defending private life and human rights,

Arguably, in all these possible roles and types of interventions lawyer must always consider in the concret case the relation between data subjet's rights and the new controller's/processor's obligations.

The core rules well known from Data Protection Directive 95/46/EC are retained in this new Regulation however often modified and expanded. Aims ? To cater for constantly changing technical environment and to introduce more consistent legal framework as regards personal data. On the one hand the Regulation is intended to address those challenges by reinforcing personal data privacy and security on the other hand its goal is to simplify the free flow of personal data in

the EU. Consequences ? Among others new or modified range of obligations to comply with for controllers but also for processors.

Paying attention to the new or modified spheres of obligations under GDPR is crucial both from the point of view of ensuring and demonstrating accountability and also from the other perspective – analysing if any data subject's right was violated. Unfulfillement in that field exposes controller and processor to the variaty of more severe remedies, liability and penalties that those which were possible under Directive – they are now set out in chapter VIII of GDPR.

(I) Most important modifications in controller's/processor's obligations:

1. Obligations connected with **expanded territorial reach of the regulation**, it will be especially important representing Clients outside from EU because such Client not established formally in EU may be caught by GDPR anyway with all consequences resulting from the necessity of compliance with GDPR. That extra-territorial scope is set out in Article 3 and in now of a statutory character – before it was rather CJEU that broaden the territorial scope of the Directive – I mean here Weltimmo case (C-230/14) and especially Google Spain (C-131/12).

   Article 3 paragraph 2 of GDPR states that:

   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: (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.

   So controller or processor can be caught by the GDPR regardless their seat if only their processing activities aims at individuals or their behaviour in the Union.

2. Introduction of the obligations also **on data processors**, that's why everywhere before and after in this presentation I do underline that we're discussing here both controller's and processor's obligations.

3. New obligations connected with obtaining a consent, also in connection with a particular protection of children,
4. Right to be forgotten – in other words right to erasure,
5. Right to data portability,
6. Modifications in information obligations, including those concerning profiling,
7. Data protection by design and by default standards,
8. Carrying out data protection impact assessment,
9. Records of data processing,
10. Rules of appointing data protection officer,
11. Data breach notifications,
12. Modified rules of data transfers outside the EU,
13. New obligations as for the contracts to process personal data between controller and processor.

I will focus now on that last issue - **contracting to proces personal data so relation between a controller and a processor, and also between a processor and further processor** if applicable. It is an important practical issue because of the very broad notion of processing and as a result the necessity to conclude such contracts very often in business relations e.g. while outsorcing, using serivces of cloud or hosting providers, accounting services, in human ressources etc.

A very **definition of processing** is mostly retained relative to the Directive. It does mean *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* (art. 4 (2)).

'**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 (art. 4 (7),*

whereas **'processor'** means *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*; (art. 4 (8)).

As it was underlined before, a big change of the new Regulation is that the act will be **directly applicable to processors**, so certain providers will be much more weighted down by finding an appriopriate compliance solution.

The Regulation retains the obligation of **written contract** between contractors and processors. However a **list of provisions that both parties must include in their contract has been expended relative to Directive**. The proper construction of the contract falls in fact on both controllers and processors. Also their liability for individuals' compensation claims will be jointly and severally.

What's more, a chosen **processor should meet all of the requirement of the Regulation**, which again, is quite a step change in relations controller-processor from the point of view of the Directive which only obliged controllers to confirm that the processors had the adequate data security level.

Citing **recital (81)** to ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, **when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing.** The adherence of the processor to **an approved code of conduct or an approved certification mechanism** may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed **by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject- matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject.** The controller and processor may choose to use **an individual contract** or **standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission.** After the completion of the processing on behalf of the controller, **the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject**.

The articles of the Regulation consequently repeat and precise those obligations :

Article 28 sets out the most important obligations connected with relations controller- procesor and the requirement regarding what should be inculed in their contractual provisions.

Art. 28

Processor

1.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**.

2.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**.

3.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:

(so we have here some mandatory obligations/provisions which must be included in data procesor contracts)

(a) 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;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32 (*that stipulates the basic regulation of the security measures for controllers but also processors*)

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) 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;

(f) 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;

(g) 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; (that i san interesting issue from the point of view of the legal relations between controller and processor – namely afted having deleted or returning the data and their copy it may be hard to proove that the contract between the parties was correctly perfomed, so in the economic relations practice it may be necessary to ask controller to issue a document/a certificate confirming that the service was well perform by the provider (processor) in case of possible future claims in cas od the conflict between parties.

(h) 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.

4.Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data

protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5.Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6.Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7.The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8.A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9.The contract or the other legal act referred to in paragraphs 3 and 4 **shall be in writing, including in electronic form.**

10.Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of the controller or procesor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Such broad processor's (e.g. service provider) obligations and restrictions might cause their willingness to search such contactual provisions that shift some liability back to the controller (consumer) on the basis of kind of cross-indemnities, when the sanction is due to controller (the case of custumer failing).

So, in conclusion the obligations of the processors under GDPR as follows:

- art. 27 to appoint a representative if based outside of the Union,

- art. 28 (3) to ensure certain minimum provisions in contracts with controllers,

- art. 28 (2), (4) not to appoint sub-processor without specific or general authorisation of the controller and to ensure there is a contract with that sub-processor that contains minimum provisions introduced by the Regultion,

- art. 29 process the data only on the instructions of the controller unless required to do it for other purposes by Union and Member State law,

- art. 30 to keep record of processing carried out on behalf of a controller,

- art. 31 to cooperate with the supervisory authorities,

- art. 32 to implement appropriate security meausures,

- art. 33 (2) notifcation to the controller of any personal data breach without undue delay

- art. 37 to appoint a data protection oficer if appliable,

- art. 44 to comply with the rules on transfer of personal data outside of the EU

There is no express grandfathering of existing processing contacts so any actual templates should be revised to ensure compliance with the Regulation while using them after May 2018. Consequently existing contracts should be amended after this date to comply with the Regulation.

(II) Additional aspects what may help analysing the new controller's/processor's obligationas

1. As it was said in the very begining, the intention of the GDPR was to make legal basis for data protection in EU more consistent. That's why the legal form od Regulation that is directly effective in all Memebr States generally without a need for further national legislation. **But in fact there will be not full harmonisation because some national divergences are inevitable.** On the basis of the very Regulation Member states have basically **right to amend** certain obligations under that act – so again from legal analysis point of view there may

be still a **nessecity to include both GDPR and national jurisdiction while working on the case**. The most crucial **national derogation's areas** concern the following:

- Member states may provide for further restrictions than those set out in the Regulation as regards processing the employees data - so labour law, art. 88.

Article 88 Processing in the context of employment

1.Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2.Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3.Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

- data subjects' rights under the Regulation can be on the other hand limited in the field of national security, crime, and judicial proceedings - art. 23,

Article 23

Restrictions

1.Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) 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;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2.In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to: (a) the purposes of the processing or categories of processing; (b) the categories of personal data; (c) the scope of the restrictions introduced; (d) the safeguards to prevent abuse or unlawful access or transfer; (e) the specification of the controller or categories of controllers; (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; (g) the risks to the rights and freedoms of data subjects; and (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

- the Regulation can be amended by Member States to reconcile data protection values with freedom of information, in order to protect information subject to professional secrecy and also to restrict the processing of national identity numbers (art. 85-91 concern that and they covers such areas as processing for journalistic and academic purposes, artistic or literary expression, public access to official documents, processing for archiving purposes in the public interest, scientific, historical and statistical research purposes, but we're also talking here about adopting specific measures in relation to controllers or processors that are subject to an obligation of professional secrecy, but data protection rules of churches and religious associations too.

Article 85

Processing and freedom of expression and information

1.Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

2.For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3.Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to

which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1.Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner. 2.Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. 3.Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. 4.Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1.Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only

with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2.Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations 1.Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation. 2.Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

- Member states can also decide that the appointment of a data protection oficer will be always mandatory (art. 37 paragraph (4)):

Article 37

Designation of the data protection officer

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 pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2.A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3.Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4.In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5.The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6.The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract. 7.The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

- as regards children – the age at which they can provide valid consent online may be reduced from 16 to 13 (art. 8.):

Article 8

Conditions applicable to child's consent in relation to information society services

1.Where point (a) of Article 6(1) applies, 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.

2.The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3.Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

- whereas, article 6 (1)c states that the compliance with an obligation under Union or Member State law is one of the justification of data processing:

Article 6

Lawfulness of processing

1.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. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2.Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX. 3.The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: (a) Union law; or (b) Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4.Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

- according to art. 10 the information about criminal offences can be processed only if it is authorised by Union or Member State law or under the control of an official authority:

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

- art. 17 states that the right to be forgotten does not apply if the processing is necessary for compliance with a legal obligation under Union or, again, Member State law:

Article 17

Right to erasure ('right to be forgotten')

1.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: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) 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; (c) 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); (d) the personal data have been unlawfully processed; (e) 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; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2.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.

3.Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information; (b) 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; (c) 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); (d) 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 (e) for the establishment, exercise or defence of legal claims.

- art. 49 (4) and (5) - Member States may introduce additional restrictions on transfers outside of the EU and on the other hand, a public interest recognised under Member States law can constitue a basis to such a transfer

2. Besides of those areas of flexibility that Member States are granted under GDPR, another challange while working with the Regulation and capturing properly the controllers and processors obligations is **often principle-base character of GDPR.** Such type of regulation gives again - some **flexibility** while applying it. However it **causes also a risk of legal uncertainty and of different interpretation in different EU countries.** For instance - art. 35 – a privacy impact assessment must be carried out where „systematic and extensive evaluation" of individuals resulting in legal effects or significantly affects those individuals. So the proper interpretation of that quite obscure notion is crucial for a proper recognition of one of the important controller's obligations under GDPR. Another example - art. 37 introduces a notion of „large scale" monitoring individuals – it is quite vague as concept but highly important from the point of view of the obligation of appointment of the DPO.

General and often uncertain character and meaning of some GDPR concepts requires paying special attention to the **guidance from supervisory authority** and of the new institution that replaces The Article 29 Working Party – namely **European Data Protection Board**.

3. Other difficulty results from the structure of the act – the Regulation consists of the articles (99) and (173) recitals. Traditionally the recitals have no biding legal force, they are just hepling in interpretation of the act, however their nature in GDPR is sometimes most unclear. For instance, the regulation

concerning consent is not very extensive in articles but very important details regarding e.g. a ban on the use of pre-ticked boxes and on tying of consent to the performance of a contract are in recitals (32,42,43). Another problem – the regulation in reciatals and lack of a proper regulation in the articles. It is the case of a representative liability. Generally entity based outside the EU must appoint a representative in EU. In the recital (80) there is a regulation that the enforcement action can be taken directy against a representative, but there is not such regulation in articles. So in practice we can encounter such problem of legal existence of the representative's liability which cannot be solved in a different way than by the judgement of CJUE because of the problem of the interpretation of the GDPR.