



### Foreword from the Chair of the ICC Commission on the Digital Economy

Paris, 1 April 2016

The International Chamber of Commerce (ICC) policy inventory on the European Union (EU) General Data Protection Regulation (GDPR) identifies aspects of the GDPR that will benefit from business experience and expertise. The tool will serve as a key resource for the global business community, who are currently scoping out how to consider and implement key aspects of the new regulation, which covers privacy and data protection for EU citizens.

Expected to be published in July of this year followed by a two year implementation process, the GDPR is generating a roar of discussion throughout the business world and once in place, will significantly affect business activity in all sectors, well beyond the borders of the EU. Including provisions on the right to erasure, binding corporate rules, and data breaches, the regulation will transform the privacy landscape known today.

To facilitate analysis of where global business input on the regulation will be most useful, ICC's Commission on the Digital Economy is publishing its inventory to make it widely available. It will be used to identify where further guidance or implementing regulations will be promulgated and to convene global business input on those articles of the regulation where business practical experience and expertise could offer most insight. ICC hopes it will encourage other business organizations to work collectively on implementation cooperatively to cover all topics that need to be addressed to maximize the benefit to our collective memberships.

The GDPR replaces Directive 95/46/EC which was enacted in 1995, and will significantly change EU data protection laws. Once officially adopted by the European Parliament and the Council of the European Union, it will apply in EU Member States after a period of two years. During a two year implementation period additional guidance is expected including whether and how Article 29 Working Party could transform into the European Data Protection Board.

The ICC Commission on the Digital Economy invites the global business community to use this inventory and hopes it proves a useful resource.

Yours sincerely,

Joseph Alhadeff

Chair ICC Commission on the Digital Economy

# Contents

<b>Foreword from the Chair of the ICC Commission on the Digital Economy.....</b>	<b>1</b>
<b>Implementing Acts.....</b>	<b>3</b>
Civil Liability.....	3
Codes of Conduct.....	3
Consent.....	4
Derogations.....	5
Freedom of Expression.....	5
Processing.....	6
Sanctions.....	11
Other.....	11
<b>Delegated Acts.....</b>	<b>13</b>
BCRs.....	13
Codes of Conduct.....	13
Processing.....	14
Other.....	14
<b>GDPR articles to consider.....</b>	<b>15</b>
Adequacy.....	15
BCRs.....	16
Certification.....	16
Codes of Conduct.....	16
Data Breach.....	17
Derogation.....	18
Fines.....	18
Right to be forgotten.....	20
Processing.....	20
Profiling.....	21
Standard clauses.....	22
Other.....	22
<b>Articles to follow up in Spring.....</b>	<b>22</b>

## International Chamber of Commerce (ICC) European Union (EU) General Data Protection Regulation (GDPR) inventory

**IMPLEMENTING ACTS** (Responsibility for implementing legally binding EU acts lies primarily with EU countries. However, some legally binding EU acts require uniform conditions for the implementation. In these cases, the Commission or, in duly justified specific cases and in cases provided in the Articles 24 and 26 of the Treaty on European Union, the Council is empowered to adopt implementing acts (Article 291 of the TFEU).

Theme	Article	Para	Extract
<b>Civil liability</b>	<b>Article 76</b> "Representation of data subjects"	1	<i>The data subject shall have the right to mandate a body, organisation or association, which has been properly constituted according to the law of a Member State, which is of non-profit making character, and whose statutory objectives are in the public interest and which is active in the field of the protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 73, 74 and 75 on his or her behalf and to exercise the right to receive compensation referred to in Article 77 on his or her behalf if provided for by Member State law.</i>
		2	<i>Member States may provide that anybody, organisation or association referred to in paragraph 1, independently of a data subject's mandate, shall have in such Member State the right to lodge a complaint with the supervisory authority competent in accordance with Article 73 and to exercise the rights referred to in Articles 74 and 75 if it considers that the rights of a data subject have been infringed as a result of the processing of personal data that is not in compliance with this Regulation.</i>
<b>Codes of conduct</b>	<b>Preamble</b>	131	<i>The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country or a territory or a processing sector within that third country or an international organisation; adopt standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board given that those acts are of general scope.</i>

	<b>Article 52</b> "Tasks"	all	<i>Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory ga) encourage the drawing up of codes of conduct pursuant to Article 38 and give an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 38 (2); gb) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 39(1), and approve the criteria of certification pursuant to Article 39 (2a);</i>
<b>Consent</b>	<b>Article 8</b> "Conditions applicable to child's consent in relation to information society services"	1	<i>Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 16 years, or if provided for by Member State law a lower age which shall not be below 13 years, shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child.</i>
	<b>Preamble</b>	8	<i>This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of sensitive data. To this extent, this Regulation does not exclude Member State law that defines the circumstances of specific processing situations, including determining more precisely the conditions under which processing of personal data is lawful.</i>
<b>Derogations</b>	<b>Article 44</b> "Derogations for specific situations"	1(g)	<i>In the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case;</i>
		5	<i>The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject.</i>
		5(a)	<i>In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.</i>

<b>Freedom of expression</b>	<b>Article 80</b> "Processing of personal data and freedom of expression and information"	1	<i>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 the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression.</i>
		2	<i>For the processing of personal data carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from the provisions in 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 organizations), Chapter VI (independent supervisory authorities), Chapter VII (co-operation 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.</i>
		3	<i>Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.</i>
<b>Processing</b>	<b>Article 6</b> "Lawfulness of processing"	3a	<i>(new) Where the processing for another purpose than the one for which the 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 points (aa) to (g) of Article 21(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the data are initially collected, take into account, inter alia: (...) (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.</i>
		2a	<i>(new) Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to the processing of personal data for compliance with Article 6(1)(c) and (e) 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.</i>
	<b>Article 9</b> "Processing of special categories of personal data"	1	<i>The processing of personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation shall be prohibited.</i>

		2	<p>Paragraph 1 shall not apply if one of the following applies:</p> <p>(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or</p> <p>(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union law or Member State law or a collective agreement pursuant to Member State law providing for adequate safeguards for the fundamental rights and the interests of the data subject; or</p> <p>(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or</p> <p>(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking 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 data are not disclosed outside that body without the consent of the data subjects; or</p> <p>(e) the processing relates to personal data which are manifestly made public by the data subject; or</p> <p>(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or</p> <p>(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; or</p> <p>(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health professional and subject to the conditions and safeguards referred to in paragraph 4; or</p> <p>(hb) 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 law 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; or</p> <p>(i) processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(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.</p> <p>(j) (...)</p>
		3	(...)



		4	<i>Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.</i>
		5	<i>Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data.</i>
	<b>Article 9a</b> "Processing of data relating to criminal convictions and offences"		<i>Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) may only be carried out either under the control of official authority or when the processing is authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions may be kept only under the control of official authority.</i>
	<b>Article 26</b> "Processor"	2(a)	<i>The carrying out of processing by a processor shall 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 purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and stipulating in particular that the processor shall: (a) process 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 the data, unless that law prohibits such information on important grounds of public interest;</i>
		2(c)	<i>take all measures required pursuant to Article 30;</i>
		2(g)	<i>at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of data processing services, and delete existing copies unless Union or Member State law requires storage of the data;</i>
		2(h)	<i>make 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. The processor shall immediately inform the controller if, in his opinion, an instruction breaches this Regulation or Union or Member State data protection provisions.</i>

		2a	<i>Where a processor enlists 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 2 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 way 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.</i>
	<b>Article 80a</b> "Processing of personal data and public access to official documents"		<i>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 law 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</i>
	<b>Article 80b</b> "Processing of national identification number"		<i>Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In this 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.</i>
	<b>Article 82</b> "Processing in the employment context"	1	<i>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.</i>
2a		<i>Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</i>	



	<b>Article 83</b> "Safeguards and derogations for the processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes"	2	<i>Where personal data are processed for scientific and historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 17a and 19 subject to the conditions and safeguards referred to in paragraph 1 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 these purposes.</i>
		3	<i>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, 17a, 17b, 18 and 19 subject to the conditions and safeguards referred to in paragraph 1 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 these purposes.</i>
<b>Sanctions</b>	<b>Article 53</b> "Powers"	4	<i>Each Member State may provide by law that its supervisory authority shall have additional powers than those referred to in paragraphs 1, 1b and 1c. These exercises of these powers shall not impair the effective functioning of the provisions of Chapter VII.</i>
	<b>Preamble</b>	119	<i>(119) Member States may lay down the rules on criminal sanctions for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. These criminal sanctions may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal sanctions for infringements of such national rules and of administrative sanctions not lead to the breach of the principle of ne bis in idem, as interpreted by the Court of Justice of the European Union.</i>
	<b>Article 78</b> "Penalties"	3b	<i>53(1b), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.</i>
<b>Other</b>	<b>Article 42</b> "Transfers by way of appropriate safeguards"	5b	<i>Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2.</i>
	<b>Article 55</b> "Mutual assistance"	4(b)	<i>Compliance with the request would be incompatible with the provisions of this Regulation or with Union or Member State law to which the supervisory authority receiving the request is subject.</i>

	<b>Article 84</b> "Obligations of secrecy"	1	<i>Member States may adopt specific rules to set out the powers by the supervisory authorities laid down in points (da) and (db) of Article 53(1) in relation to controllers or processors that are subjects 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. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.</i>
		2	<i>Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.</i>

**DELEGATED ACTS** (Article 290 of the TFEU allows the EU legislator (generally, the European Parliament and the Council) to delegate to the Commission the power to adopt non-legislative acts of general application that supplement or amend certain non-essential elements of a legislative act)

Theme	Article	Para	Extract
<b>BCRs</b>	<b>Article 43</b> "Transfers by way of binding corporate rules"	4	<i>The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</i>
<b>Codes of conduct</b>	<b>Article 38</b> "Codes of conduct"	2b	<i>Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards.</i>
		4	<i>The Commission may adopt implementing acts for deciding that the approved codes of conduct and amendments or extensions to existing approved codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</i>
	<b>Article 39a</b> "Certification body and procedure"	7	<i>The Commission shall be empowered to adopt delegated acts in accordance with Article 86, for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1 of Article 39.</i>
		8	<i>The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).</i>

<b>Processor</b>	<b>Article 26</b> "Processor"	2b	<i>The Commission may lay down standard contractual clauses for the matters referred to in paragraph 2 [The carrying out of processing by a processor shall 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 purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the controller and stipulating in particular that the processor shall...] and 2a [Where a processor enlists 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 2 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 way 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.] and in accordance with the examination procedure referred to in Article 87(2). [Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.]</i>
	<b>Article 41</b> "Transfers with an adequacy decision"	4a	<i>The Commission shall, on an on-going basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.</i>
<b>Other</b>	<b>Article 12</b> "Transparent Information, communication and modalities for exercising the rights of the data subject"	4c	<i>The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.</i>
	<b>Article 55</b> "Mutual assistance"	10	<i>The Commission may specify the format and procedures for mutual assistance referred to in this article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).</i>
	<b>Article 58</b> "Opinion by the European Data Protection Board"	1(cb)	<i>The European Data Protection Board shall issue an opinion whenever a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the European Data Protection Board, when it:...aims at approving the criteria for accreditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to paragraph 3 of Article 39a; or</i>

## GDPR articles to consider

(these are articles may or may not be implementing or delegated acts but may have important consequences for business thus are flagged for consideration)

Theme	Article	Para	Extract
<b>Adequacy</b>	Preamble	87	<i>In the absence of an adequacy decision, Union law or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organization.</i>
	Article 41 "Transfers with an adequacy decision"	3	<i>The Commission, after assessing the adequacy of the level of protection, may decide that a third country, or a territory or one or more specified sectors within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectorial application and, where applicable, identify the supervisory authority or authorities mentioned in point(b) of paragraph 2. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2).</i>
		5	<i>The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3, decide that a third country, or a territory or a specified sector within that third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 and, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 without retro-active effect. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency, in accordance with the procedure referred to in Article 87(3).</i>
		8	<i>Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5.</i>
<b>BCRs</b>	Article 53 "Powers"	1c (d)	<i>Each supervisory authority shall have the following authorisation and advisory powers... : (d) to approve binding corporate rules pursuant to Article 43.</i>

<b>Certification</b>	<b>Article 39</b> "Certification"	all	<p><i>1 The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations carried out by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.</i></p>
<b>Codes of conduct</b>	<b>Article 34</b> "Prior consultation"	all	<p><i>2. The controller shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.</i></p> <p><i>3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 would not comply with this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, it shall within a maximum period of eight weeks following the request for consultation give advice to the data controller, and where applicable the processor in writing, and may use any of its powers referred to in Article 53. This period may be extended for a further six weeks, taking into account the complexity of the intended processing. Where the extended period applies, the controller, and where applicable the processor shall be informed within one month of receipt of the request including of the reasons for the delay. These periods may be suspended until the supervisory authority has obtained any information it may have requested for the purposes of the consultation..</i></p> <p><i>6. When consulting the supervisory authority pursuant to paragraph 2, the controller shall provide the supervisory authority with</i></p> <p><i>(a) where applicable, the respective responsibilities of controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings; (b) the purposes and means of the intended processing; (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation; (d) where applicable, the contact details of the data protection officer; (e) the data protection impact assessment provided for in Article 33; and (f) any other information requested by the supervisory authority</i></p>



	<p><b>Article 38</b> "Codes of Conduct"</p>	<p>all</p>	<p><i>1 The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors and the specific needs of micro, small and medium-sized enterprises.</i></p> <p><i>2 1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as:</i></p> <p><i>(a) fair and transparent data processing;(aa) the legitimate interests pursued by controllers in specific contexts(b) the collection of data</i></p> <p><i>2b. Where the draft code of conduct relates to processing activities in several Member States, the supervisory authority competent pursuant to Article 51 shall, before approval, submit it in the procedure referred to in Article 57 to the European Data Protection Board which shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation or, in the situation referred to in paragraph 1ab, provides appropriate safeguards.</i></p> <p><i>3 Where the opinion referred to in paragraph 2b confirms that the codes of conduct, or amended or extended codes, is in compliance with this Regulation, or, in the situation referred to in paragraph 1ab, provides appropriate safeguards, the European Data Protection Board shall submit its opinion to the Commission.</i></p>
<p><b>Data breach</b></p>	<p><b>Article 66</b> "Tasks of the European Data Protection Board"</p>	<p>1 bb</p>	<p><i>bb)(new) issue guidelines, recommendations and best practices in accordance with point (b)f Article 66(1) for establishing the data breaches and determining the undue delay referred to in paragraphs 1 and 2 of Article 31 and for the particular circumstances in which a controller or a processor is required to notify the personal data breach; bc)(new) issue guidelines, recommendations and best practices in accordance with point (b)of Article 66(1) as to the circumstances in which a personal data breach is likely to result in a high risk for the rights and freedoms of the individuals referred to in Article 32(1).</i></p>

<p style="text-align: center;"><b>Derogations</b></p>	<p><b>Article 44</b> "Derogations for specific situations"</p>	<p style="text-align: center;">1</p>	<p><i>In the absence of an adequacy decision pursuant to paragraph 3 of Article 41, or of appropriate safeguards pursuant to Article 42, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: Derogations (consent, contracts, compelling legitimate interest etc. Recommendations and best practices to further specify the criteria and requirements for transfers based on explicit consent, contractual necessity, public interest and "compelling legitimate interest".</i></p> <p><i>1(h) Where a transfer could not be based on a provision in Articles 41 or 42, including binding corporate rules, and none of the derogations for a specific situation pursuant to points (a) to (g) is applicable, a transfer to a third country or an international organisation may take place 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, where the controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall in addition to the information referred to in Article 14 and Article 14a, inform the data subject about the transfer and on the compelling legitimate interests pursued by the controller.</i></p>
<p style="text-align: center;"><b>Fines</b></p>	<p><b>Article 79</b> " General conditions for imposing administrative fines "</p>	<p style="text-align: center;">5</p>	<p><i>5 Where the legal system of the Member State does not provide for administrative fines, Article 79 may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that these legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. These Member States shall notify to the Commission those provisions of their laws by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.</i></p>
<p style="text-align: center;"><b>Right to be forgotten</b></p>	<p><b>Article 17</b> "Right to be erasure ("right to be forgotten")"</p>	<p style="text-align: center;">all</p>	<p><i>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:</i></p> <p><i>(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</i></p> <p><i>(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 of the data;</i></p> <p><i>(c) the data subject objects to the processing of personal data pursuant to Article 19(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of personal data pursuant to Article 19(2);</i></p> <p><i>(d) they have been unlawfully processed;</i></p> <p><i>(e) the data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;</i></p> <p><i>(f) the data have been collected in relation to the offering of information society services referred to in Article 8(1).</i></p> <p><i>1a. (...)</i></p>

<b>Processing</b>	<b>Article 33</b> "Data protection impact assesment"	2a	<i>The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the European Data Protection Board.</i>
		2b	<i>The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the European Data Protection Board.</i>
		2c	<i>Prior to the adoption of the lists referred to in paragraphs 2a and 2b the competent supervisory authority shall apply the consistency mechanism referred to in Article 57 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.</i>
		3	<i>The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including where applicable the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.</i>
		5	<i>Where the processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law, or the law of the Member State to which the controller is subject, and such law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been made as part of a general impact assessment in the context of the adoption of this legal basis, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.</i>
<b>Profiling</b>	<b>Article 66 g</b> "Tasks of the European Data Protection Board"	1	<i>(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation; (ba)(new) issue guidelines, recommendations and best practices in accordance with point (b) of Article 66(1) for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 20(2);</i>

<b>Standard clauses</b>	<b>Article 42</b> "Transfers by way of appropriate safeguards"	2	<p>The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:</p> <p>(oa) a legally binding and enforceable instrument between public authorities or bodies; or</p> <p>(a) binding corporate rules in accordance with Article 43; or</p> <p>(b) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 87(2); or</p> <p>(c) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 87(2); or</p> <p>(d) an approved code of conduct pursuant to Article 38 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</p> <p>(e) an approved certification mechanism pursuant to Article 39 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.</p>
		5b	<p>Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with p 2.</p>
<b>Other</b>	<b>Preamble</b> impact assessments	66a	<p>The controller should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of this risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data is in compliance with this Regulation. <u>Where a data protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.</u></p>
	<b>Article 37</b> "impact assessment"	1	<p>Tasks of the data protection officer</p> <p>1. The data protection officer shall have at least the following tasks:</p> <p>(a) to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;</p> <p>(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awarenessraising and training of staff involved in the processing operations, and the related audits;(c) (...)</p> <p>(d) (...) (e) (...)</p> <p>(f) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 33;</p>

	<b>Article 45</b> "International co-operation for the protection of personal data"	all	<i>1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to: (a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data; (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.</i>
	<b>Article 66 "</b> Tasks of the European Data Protection Board"	all	<i>ab) (new) issue guidelines, recommendations, and best practices on procedures for deleting links, copies or replications of personal data from publicly available communication services as referred to in Article 17 paragraph 2; 4.a The European Data Protection Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.</i>
	<b>Distance Selling Issues in the Website Context Preamble</b>	para20	<i>In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects irrespective of whether connected to a payment or not. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller is envisaging the offering of services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's or an intermediary's website in the Union or of an email address and of other contact details or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, and/or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to such data subjects in the Union.</i>
	<b>Article 84</b> "Obligations of secrecy"	1	Member States may adopt specific rules to set out the powers by the supervisory authorities laid down in points (da) and (db) of Article 53(1) in relation to controllers or processors that are subjects 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. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy.

## GDPR Articles to follow up in Spring (these articles are in the regulation but not finalised)

Article	Para	Potentially
Article 8 "Conditions applicable to child's consent in relation to information society services"	3	delegated act
Article 9 "Processing of special categories of personal data"	3	delegated act
Article 26 "Processor"	5	delegated act
Article 43 "Transfers by way of binding corporate rules"	3	delegated act
Article 79a	4	delegated act
Article 8 "Conditions applicable to child's consent in relation to information society services"	4	implementing act
Article 12 "Transparent information, communication and modalities for exercising the rights of the data subject"	6	implementing act
Article 14 "Information to be provided where the data are collected from the data subject"	8	implementing act
Article 15 "Right of access for the data subject"	4	implementing act
Article 18 "Right to data portability"	3	implementing act
Article 23 "Data protection by design and by default"	4	implementing act
Article 28 "Records of processing activities"	6	implementing act



<b>Article 30</b> "Security of processing"	4	implementing act
<b>Article 31</b> " Notification of a personal data breach to the supervisory authority'	6	implementing act
<b>Article 32</b> " Communication of a personal data breach to the data subject"	6	implementing act
<b>Article 34</b> "Prior consultation"	9	implementing act
<b>Article 41</b> "Transfers with an adequacy decision"	3a	implementing act
<b>Article 62</b> "Exchange of information"	2	implementing act
	1a	implementing act
	1b	implementing act
	1c	implementing act