Conciliating data protection and legal certainty:
In support of a data protection Regulation fit for SMEs[1]

Clarity: SMEs need simple and clear rules. The proposed Regulation currently holds dispositions for SMEs dispersed across 10 articles directly (and 44 articles indirectly) in the text. This fails to live by the EC standards expressed in the Smart Regulation of October 2010, where the Commission committed to limit the regulatory burden for SMEs to what is strictly necessary. The proposed Regulation is clearly not fulfilling the promise made to SMEs. **We request one article covering the duties for SMEs**, to ensure SMEs can clearly establish their responsibilities.

Certainty: ACT and ESBA share the concerns of stakeholders and Member States relative to delegated acts. SMEs need legal certainty in order to guarantee investments made and forward looking strategies. As such, **any article pertaining to SMEs' obligations should feature definite rules**. SMEs already suffer from an uncertain economic landscape, they cannot afford legal jeopardy. We set out below our suggestion on how the regulation should address the obligation of SMEs with regard to data protection.

Simplicity: Supervisory authorities have the necessary expertise and means to assess user rights and potential infringements. As such, they should be the first point of call for the user rather than the SME itself. In order to simplify the procedure relative to requests from data subjects on the processing of their information and with regard to the limited material and human resources available to the SMEs, it makes sense for the Data Protection Authorities (DPAs) to be the first port of call for consumers as they are best placed to exercise a judgement on the issue of concern.

With reference to the above mentioned on legal clarity, certainty and simplicity, ACT[2] and ESBA request one article for SMEs containing modified elements of the present text. This to ensure that SMEs are given a legal framework that is definite, understandable and manageable.

[1] 1. The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.
2. Within the SME category, a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.
3. Within the SME category, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.
Source: EurLex Commission recommendation C(2003) 1422

[2] ACT is also part of the Internet Coalition on Data Protection. As such it has signed up to positions to ensure that EU policy-makers reflect on certain articles that could damage the online ecosystem and business models whilst not providing consumers with greater trust. The present paper is complementary and not *in lieu* of supported positions.

Note to reader: text written in ***bold italic*** represents new amendments. Text in cut cross ~~(cut cross)~~ is the original Regulation proposal text to be deleted. Entire points or paragraphs deleted from the Regulation proposal are mentioned in the left column.

Amendment of current articles (in numerical order) establishing a single article regulating the responsibility of SMEs

SME processing of a personal data of a child

Modification of Article 8

Paragraph 3 replaced with new text and paragraph 4 deleted entirely.

1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a ***data subject known to be of age under 13*** ~~child below the age of 13 years~~ shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. ~~The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.~~ ***SME controllers shall make reasonable efforts to obtain the verifiable consent of a child's parent or custodian before processing personal data of a data subject known to be of age under 13. The efforts undertaken should be assessed taking into consideration the limited financial, material and human resources available to micro and small enterprises. As such, reasonable effort will be satisfied by way of electronic communication to the email provided. Where this notification is not answered, consent will not be granted.***

2. 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.

3. ***SME controller shall not be held liable for any fraudulous data entry or requirements to verify user identity.***

Modification of Article 12

Paragraphs 5 and 6 deleted entirely.

SME processing of procedures and mechanisms for exercising the rights of the data subject

1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.

2. The controller shall inform the ~~data subject~~ ***supervisory authority*** without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing ***and***. ~~Where the data subject makes the request in electronic form~~, ~~the information shall be~~ provided in electronic form, ~~unless otherwise requested by the data subject.~~

3. If the controller refuses to take action on the request of the ~~data subject~~ ***supervisory authority***, the controller shall inform the ~~data subject~~ ***supervisory authority*** of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.

SME provision on information to the data subject

Modification of Article 14

Points 1.(h) 3,7 and 8 deleted entirely.

1. Where personal data relating to a data subject are collected, the controller shall provide the ~~data subject~~ ***supervisory authority*** with ~~at least~~ the following information:

(a) the identity and the contact ~~details~~ email of the controller and, if any, of the controller's representative ~~and of the data protection officer~~;

(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

(c) the ***expected*** period for which the personal data will be stored;

(d) the existence of the right to request from the ~~controller~~ ***supervisory authority to request of the SME*** access to and rectification or erasure of the personal data, ***where data is core to the business of the SME***, concerning the data subject or to object to the processing of such personal data;

(e) the ~~right to lodge~~ ***requirements for*** a ***query and or a*** complaint to ***be lodged via*** the supervisory authority and the contact details of the supervisory authority;

(f) ***where known to the SMEs and where specifically requested***, the recipients or categories of recipients of the personal data;

(g) where ***known*** and applicable, ***and where treatment of data is core to the business of the SME***, that the controller intends to transfer to a third country or international organisation ~~and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;~~

2. Where the personal data are collected from the data subject, the controller shall inform the data subject, ***by way of change to terms and conditions***, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.

4. The controller shall provide the information referred to in paragraphs 1 and 2 and ~~3:~~

(a) at the time when the personal data are obtained from the data subject; or

(b) ~~where the personal data are not collected from the data subject, at the time of the recording or~~ within a reasonable period after the collection, ~~having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed~~.

5. Paragraphs 1 to 4 shall not apply, where:

(a) the data subject has already the information referred to in paragraphs 1, 2 ~~and 3;~~ or

(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort; or

(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or

(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.

6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.

SME provision on Responsibility of the controller

Modifications of Article 22

Point 4 deleted entirely.

1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

2. The measures provided for in paragraph 1 shall in particular include:

(a) keeping the documentation pursuant to Article 28;

(b) implementing the data security requirements laid down in Article 30;

(c) performing a data protection impact assessment pursuant to Article 33;

(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);

(e) designating a data protection officer pursuant to Article 35(1).

3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures referred to in paragraphs 1 and 2. ~~If proportionate, this verification shall be carried out by independent internal or external auditors~~.

SME provision on Representatives of controllers not established in the Union

Modification of Article 25

1. In the situation referred to in Article 3(2), the controller shall designate a representative ~~in the Union~~.

2. This obligation shall not apply to:

(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or

(b) ~~an enterprise employing fewer than 250 persons; or~~ ***SMEs where EU sales are less than 50% of revenue; or***

(c) a public authority or body; or

(d) a controller offering only occasionally goods or services to data subjects residing in the Union.

3. ***If foreign, the SME*** ~~the~~ representative shall be established ~~in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside~~ ***where it best suits the SMEs' interest as long as he is reachable by and responsive to the supervisory authority.***

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Modification of Article 28

Point 3(b) and 3(f), 4(b) , 5 and 6 deleted entirely.

SME processing of documentation

1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of ~~all~~ processing operations under its responsibility.

2. The obligation made to the controller shall not apply to SMEs processing data only as an activity ancillary[3] to the sale of goods or services.

3. The documentation shall contain ~~at least~~ the following information:

a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;

c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

(d) ~~a description of categories of data subjects and of the categories of personal data relating to them;~~ ***a description of known personal data categories collected***

[3] Ancillary activity should be defined as business or non-trade activity that is not associated with the core activities of a firm. In relation to data protection, data processing activities which do not represent more than 50% of company's turnover shall be considered ancillary.

(e) the ***known*** recipients or categories of recipients of the personal data, ~~including the controllers to whom personal data are disclosed for the legitimate interest pursued by them~~;

(g) a general indication of the ***intended*** time limits for erasure of the different categories of data;

(h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority ***within 3 months.***

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:

a) ~~a natural person~~ ***SMEs*** processing personal data without this resulting in a commercial gain;

SME provision on security of processing

Modification of Article 30

Points 3 and 4 deleted entirely.

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation. ***Measures will be deemed appropriate if they reflect security measures undertaken in products and service deemed of a similar nature. The supervisory authority shall be responsible for notifying SMEs of what it deems as state of the art.***

2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

SME processing of data protection impact assessment

Modification of Article 33

Point 2(e) and points 4, 5 and 7 deleted entirely.

1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. ***SMEs shall only be required to perform an impact assessment after their 3rd year of incorporation[4] where data processing is deemed as a core activity of their business.***

[4] Within the first three years after the establishment of a business, an average of 80% of newly established SMEs fail. Allowing this time period before the impact assessment is required will result in all businesses being given a chance to succeed before being by cost that can range in the thousands of Euros.

2. The following processing operations in particular present specific risks referred to in paragraph 1:

(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;

(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;

(d) personal data in large scale filing systems on children, genetic data or biometric data;

3. The assessment shall contain ~~at least~~ a general description of the envisaged processing operations, an assessment of ~~the~~ ***most likely*** risks to the rights and freedoms of data subjects, the measures envisaged to ~~address the risks, 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~~ ***the SMEs concerned***.

SMEs processing of designation of the protection officer

Modification of Article 35

Points 1(b), 1 (c) ,3 and 11 deleted entirely.

1. The ***SME*** controller and the processor shall designate a data protection officer ~~in any case~~ ***only*** where:

(a) ~~the processing is carried out by a public authority or body; or~~ ***the treatment of data by the SME falls outside the scope of ancillary activity[5] and where the core[6] 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*.**

2~~. In the case referred to in point (b) of paragraph 1~~, a group of ***SME*** undertakings ***fitting within the above category*** may appoint a single data protection officer.

[5] See footnote 3 for relevant definition.

[6] Where 50% of annual turnover resulting from sale of data or revenue gained from this data (e.g. ad services).

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 designate a data protection officer.

5. The controller or processor shall designate the data protection officer ***as he sees fit*** ~~on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor~~.

6. The controller or the processor shall ensure that ***the data protection activities do not result in conflict of interest*** ~~any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.~~

7. The controller or the processor shall designate a data protection officer for ~~a period of at least two years~~ ***a given term period of his choosing***. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may ~~only~~ be dismissed, ~~if the data protection officer no longer fulfils the conditions required for the performance of their duties~~ ***as the company management sees fit.***

8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.

9. The controller or the processor shall communicate ***on request*** the name and contact details of the data protection officer to the supervisory authority and to the public.

10. Data subjects shall have the right to contact the ***supervisory authority to initiate a request to the SME*** ~~data protection officer~~ on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation. ***The supervisory authority will in turn be required to assess, gather and relay the information provided by the SMEs to the user(s) concerned.***

Modifications of Article 79

Point 7 deleted entirely.

SMEs processing of administrative sanctions

1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.

2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach.

3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:

(a) a natural person is processing personal data without a commercial interest; or

(b) ~~an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.~~ ***SME controller is processing personal data only as an activity ancillary to its main activity.***

4. The supervisory authority shall impose a fine ~~up to 250 000 EUR~~ ***up to 5 000 EUR***, ~~or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently~~:

(a) does not provide the mechanisms for requests by data subjects or does not respond ~~promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2)~~ ***within 3 months of requests by the supervisory authority;***

(b) charges a fee for the information or for responses to the requests of data subjects ***via the supervisory authority*** in violation of Article 12(4).

5. The supervisory authority shall impose a fine up to ~~500 000~~ ***5,000*** EUR, ~~or in case of an enterprise up to 1 % of its annual worldwide turnover,~~ to anyone who, intentionally or negligently:

(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the ~~data subject pursuant to Article 11, Article 12(3) and Article 14~~; ***via the supervisory authority.***

(b) does not provide access for the ~~data subject~~ ***supervisory authority*** or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;

(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take ~~all~~ necessary steps to inform third parties that a ~~data subjects~~ ***supervisory authority*** requests to erase any links to, or copy or replication of the personal data pursuant Article 17;

(d) does not provide a copy of the ***available and retrievable*** personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;

(e) does not ~~or not~~ sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;

(f) does not ~~or not~~ sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);

(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.

6. The supervisory authority shall impose a fine up to ~~1 000 000 EUR~~ ***5 000 EUR*** ~~or, in case of an enterprise up to 2 % of its annual worldwide turnover~~, to ~~anyone~~ ~~who~~ ***any SME which***, intentionally or negligently:

(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;

(b) processes special categories of data in violation of Articles 9 and 81;

(c) does not comply with an objection or the requirement pursuant to Article 19;

(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;

(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;

(f) does not designate a representative pursuant to Article 25;

(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;

(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;

(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;

(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;

(k) misuses a data protection seal or mark in the meaning of Article 39;

(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;

(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);

(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article 53(2);

(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.

Amendments to the dependant articles (in order of appearance)

Modifications of Article 6.

The following reflects only the changes made to the subsequent articles and paragraphs.

Point 5 deleted entirely.

Lawfulness of processing

6.1.f ***Define legitimate interest collection of any information that is necessary to the processor in so far as it enables him/her to provide an adequate and/or better service/product or can be monetized, without prejudice to the fundamental rights of the data subject, to create/add to revenue stream.***

Modifications of Article 7

Conditions of consent

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. ***Proof of consent will be satisfied by way of acceptance of the terms and conditions.***

4. ~~Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.~~

4. Consent shall not provide a legal basis for the processing, in case there is a significant imbalance between the position of the data subject and the controller. ***If the controller is an SME, the position between the data subject and the controller will be considered balanced.***

5. The Commission shall review Article 7.4 within two years of adoption of this Regulation. This review will consist of a Report on the relation between the data subject and the data controller, in cases where the data controller is an SME. If the Commission is not able to demonstrate an imbalanced relationship between the data subject and the data controller in cases where the data controller is an SME, Article 7.4 will continue to apply.

Modifications of Article 11

Transparent information and communication

2. The controller shall provide any information and any communication relating to the processing of personal data to the ~~data subject~~ ***supervisory authority*** in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.

Modifications of Article 15

Point 3 deleted entirely

Right of access for the data subject

1. The data subject shall have the right to obtain from the ~~controller~~ ***supervisory authority*** at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide ***to the supervisory authority*** the following information:

2. The data subject shall have the right to obtain from the controller ***via the supervisory authority*** communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

4. The ~~Commission~~ ***supervisory authority*** may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Modifications of Article 16

Right to rectification

The data subject shall have the right to obtain from the controller ***via the supervisory authority*** the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.

Modifications of Article 17

Right to be forgotten and to erasure

Point 9 deleted entirely

1. The data subject shall have the right to obtain from the controller ***via the supervisory authority*** the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies

2. ~~Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data.~~ Where the controller has authorised a third party publication of personal data, the controller shall ***not*** be considered responsible for that publication ***in so far as this has been communicated and consented by the data subject in the terms and conditions.***

3**.** The controller shall carry out the erasure ~~without delay~~ **within 3 months**, except to the extent that the retention of the personal data is necessary:

Modifications of Article 18

Point 3 deleted entirely

Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used ~~and allows for further use by the data subject~~.

Modifications of Article 19

Right to object

1. The data subject shall have the right to object ***to the supervisory authority***, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates ***to the supervisory authority*** compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object ***to the supervisory authority*** free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

3. Where an objection is upheld ***by the court of law*** pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.

Modification of Article 20

Point 5 deleted entirely

Measures based on profiling

Modifications of Article 23

Point 3 deleted entirely.

Data protection by design and by default

4. The ~~Commission~~ ***supervisory authority*** may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Modification of Article 26

Point 5 deleted entirely

Processor

Notification of a personal data breach to the supervisory authority

Modification of Article 31

Point 5 deleted entirely.

1. In the case of a personal data breach, the controller shall without undue delay ~~and, where feasible, not later than 24 hours after having become aware of it,~~ notify the personal data breach to the supervisory authority. ~~The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.~~

2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller ~~immediately~~ ***without undue delay*** after the establishment of a personal data breach.

3.b. ***where applicable,*** communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained;

Communication of a personal data breach to the data subject

Modification of Article 32

Point 5 deleted entirely

6. The ~~Commission~~ ***supervisory authority*** may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Modification of Article 34

Point 8 deleted entirely.

1. ***SMEs shall not be required to obtain authorisation or enter into consultation with supervisory authorities if:***

a.) ***data is ancillary (i.e. not core) to its business; or***

b.) ***it has been incorporated for less than 3 years.***

1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation. ***Failure by the supervisory authority to give a response after one month would give the SME legitimate ground to pursue.***

2. The controller or processor acting on the controller's behalf shall ~~consult~~ ***notify*** the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:

(a) ***if applicable to the SME,*** a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or

3. Where the supervisory authority is of the opinion that the intended processing does

not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall ~~prohibit the intended processing and~~ make appropriate proposals to remedy such incompliance.

6. ***Where applicable to the SME,*** the controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

9. ~~The Commission~~ ***The supervisory authority*** may set out ***or update*** standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Modification of Article 36

Position of the data protection officer

1. ***Where applicable,*** the controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.

2. ***Where applicable***, the controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.

3. ***Where applicable,*** the controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.

Modification of Article 37

Tasks of the data protection officer

1. ***Where applicable,*** the controller or the processor shall entrust the data protection officer at least with the following tasks:

2. ~~The Commission~~ ***The supervisory authority*** shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.