PRIVACY INTERNATIONAL

Summary analysis of European Commission proposal for a Data Protection Directive in the law enforcement sector

Privacy International
46 Bedford Row
London WC1R 4LR
Phone +44 (0)20 7242 2836
info@privacy.org
www.privacyinternational.org
Twitter @privacyint

September 19 2012

On 25 January 2012, the European Commission published a proposal that would comprehensively reform the European data protection legal regime. One aspect of its proposal, a new Regulation (the "Proposed Regulation"),[1] would modernise and further harmonise the data protection regime created by the Data Protection Directive (95/46/EC). Another aspect of the Commission's proposal, a new Directive (the "Proposed Directive"), would set out new rules on "the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data".[2] This paper summarises the key elements of the Proposed Directive.

Early reactions to the Proposed Directive were critical. Both the European Data Protection Supervisor ("EDPS") declared that it "does not meet the requirement of a consistent and high level of data protection".[3], and the Article 29 Data Protection Working Party ("WP29") stated that it is "disappointed by the Commission's level of ambition and [the Article 29 Working Party] underlines the need for stronger provisions".[4] It further states that, as a result of political constraints, the Proposed Directive does not mandate a sufficiently high level of data protection.

Privacy International strongly supports these conclusions and considers that the EU Commission drafters have failed in their duty to ensure a high level of data protection for EU citizens across the board, both in the private and public sector. Police and judicial cooperation in the context of law enforcement is an area where sensitive personal data is likely to be involved, and therefore citizens may be put at particular risk. We are therefore looking to the Parliament and the Council to ensure that a high level of data protection by the relevant public authorities is mandated throughout the EU.

The chart below identifies areas where data protection is not robustly mandated in the Proposed Directive; it also identifies areas where Privacy International calls for improvements that, if implemented, would make the Proposed Directive more comprehensive and more protective of individual privacy in the law enforcement context.

The chart concentrates in particular on strengthening two essential aspects in the Proposed Directive: (i) the rights of the data subject and (ii) the obligations of the controller. By doing so, it can become more in tune with the Proposed Regulation.

[1] *See* COM(2012) 11 Final, 2012/0011 (COD).
[2] *See* COM(2012) 10 Final, 2012/0010 (COD).
[3] *See* EDPS Opinion, 7 March 2012, "EDPS applauds strengthening of the right to data protection in Europe, but still regrets the lack of comprehensiveness".
[4] *See* Article 29 Data Protection Working Party Opinion, 23 March 2012, 00530/12/EN, WP 191, "Opinion 01/2012 on the data protection reform proposals".

Our five key findings reflected in this chart are:

1. **The data processing principles are less ambitious and more ambiguous than those in the Proposed Regulation.**
2. **The rights of data subjects are significantly weaker than they would be under the Proposed Regulation.**
3. **Controllers are subject to fewer, and vaguer, obligations than they would be under the Proposed Regulation.**
4. **Transfer rules are unclear, and less restrictive than they could be.**
5. **Supervisory authorities have fewer powers of oversight, and much weaker powers of interference or enforcement.**

Please note that, as defined in the Proposed Directive, references to "controller" in the chart below are references to a "competent public authority that alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law." In most cases, the chart summarises "Existing Requirements of the Proposed Directive" as if Member States have already fulfilled the requirements of the Proposed Directive. All references to "data" are references to "personal data".

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
Data Processing Principles and Lawful Processing • **The data processing principles are, on the whole, more ambiguous, more limited, and weaker than the principles set out in the Proposed Regulation.** See, in particular, Art 4 of the Proposed Directive. • **Unlike the Proposed Regulation, the Proposed Directive has no special restriction on the processing of data relating to children**. See, by contrast, Art 8 of the Proposed Regulation.		
Art 4(a). Principles relating to personal data processing - fair processing	Personal data must be processed in accordance with six data processing principles. The first principle requires that data be processed fairly and lawfully.	The first principle must also require that data be processed in a transparent manner in relation to the data subject. If necessary, to accommodate the law enforcement context, this part of the principle could be made only to apply "where possible". (This change proposes language set out in Art 5(a) of the Proposed Regulation.)

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
Art 4(b). Principles relating to personal data processing - purpose of processing	The second principle requires that data be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.	A new recital should be inserted into the Proposed Directive to clarify the meaning of an "incompatible purpose"[5].
Art 4(c). Principles relating to personal data processing - limits of processing	The third principle requires that processed data are adequate, relevant, and "not excessive in relation to the purposes for which they are processed".	(1) The words "not excessive in relation to the purposes for which they are processed" should be revised to limit processing to "the minimum necessary". (This change proposes language set out in Art 5(c) of the Proposed Regulation.) (2) The third principle should clarify that processing may only take place if, and as long as, the purpose could not be fulfilled without processing data. (This change proposes language set out in Art 5(c) of the Proposed Regulation.)
Art 4(d). Principles relating to personal data processing - up-to-date processing	The fourth processing principle states that data, "where necessary", must be kept up to date.	To make this requirement unconditional, the words "where necessary" should be removed from Art 4(d). (This change proposes language set out in Art 5(d) of the Proposed Regulation.)[6] . *Note: See also chart entries for Art 18 and 4(f) below.*
Art 5 and 6. Distinction between categories of data subject and accuracy and reliability of data	Controllers must, "as far as possible", make a clear distinction between different categories of data subject. Also, "as far as possible", controllers must ensure that different categories of data are processed in accordance with their degree of accuracy and reliability. Member States must also ensure that, "as far as possible", data based on facts are distinguished from data based on personal assessments.	To make this requirement unconditional, the language "as far as possible" should be removed from Art 5 and Art 6(1) and (2)[7].
Art 7. Lawfulness of processing	Processing of personal data is only lawful under limited circumstances. These circumstances are, however, broadly drafted.	This provision should specifically make a clear distinction between the lawfulness of processing for an initial, specific purpose, and exceptions that would allow processing for a separate, subsequent purpose.

[5] As proposed in para 331, EDPS Opinion [full citation###]
[6] As proposed in paras 327-328 EDPS Opinion
[7] As proposed on p. 27 Article 29 Working Party Opinion

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
		Any change of purpose should be required to satisfy a carve-out test of necessity and proportionality, for example (see also entry below on Art 11 of the Proposed Directive). (This change proposes language set out in Art 6(4) of the Proposed Regulation.) *Note: Unlike the Proposed Regulation, the Proposed Directive does not set out lawful grounds or safeguards for the processing of historical, statistical or scientific research.*
Processing of data relating to children	The Proposed Regulation places further restrictions on the processing of data relating to children below the age of 13 years. The Proposed Directive has no equivalent provision.	Restrictions should be included in the Proposed Directive on the processing of data relating to children under the age of 13, and a higher level of justification should be required for processing such data. (This change proposes language set out in Art 8 of the Proposed Regulation.)

Rights of the Data Subject

- **There are protections against measures based on profiling, but, unlike their peers under the Proposed Regulation, individuals have no right not to be subject to such measures.** See Art 9 of the Proposed Directive.

- **Controllers are under a duty to provide information to data subjects, but there are caveats. For example, controllers do not need to establish procedures to respond to requests if they would be required to take an "unreasonable" step. In contrast to their peers under the Proposed Regulation, controllers may be less transparent and less responsive to requests, and slower to respond. Under the Proposed Directive, controllers are not required to work with third party recipients of the data to rectify or erase data, and they will find it easier to charge data subjects a "request fee".** See Art 10 of the Proposed Directive.

- **Significant carve-outs further limit data subject access rights in comparison to the Proposed Regulation. In some cases, Member States may choose to exempt whole categories of data. Controllers are not generally required to consider whether the carve-outs apply on a case-by-case basis**. See Art 11 and 13 of the Proposed Directive.

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
• **Supervisory authorities have an oversight role in ensuring that data subject requests are complied with, but have very limited powers of enforcement**. See Art 14 of the Proposed Directive. • **Data subject rights to erasure and rectification are more limited and more ambiguous than they are under the Proposed Regulation**. See Art 15 and 16 of the Proposed Directive. • **Unlike their peers under the Proposed Regulation, data subjects do not have rights to be forgotten, rights for data portability or the right to object to processing.** See, by contrast, Art 17, 18 and 19 of the Proposed Regulation.		
Art 9. Measures based on profiling / automated processing	Automated processing that is intended to evaluate personal aspects relating to a data subject that would produce an adverse legal effect for the data subject or that would significantly affect them, must be prohibited by the Member States, unless authorised by a law that also takes measures to safeguard the data subject's legitimate interests. Automated processing cannot be based solely on the special categories of personal data specified in Art 8 of the Proposed Directive.	To strengthen the ability of individuals to enforce the prohibition on profiling and automated processing, Art 9 should be revised to give individuals a right not to be subject to such measures, in addition to the current requirement (that applies to the Member States). (This change proposes language set out in Art 20 of the Proposed Regulation.)
Art 10(3). Controllers must establish procedures to provide data subjects with information / access	Controllers must "take all reasonable steps" to establish procedures to provide data subjects with information requested under Art 11 (information to the data subject), and for the exercise of rights set out in Art 12 - 17 (data subject rights of access, rectification, erasure, etc.).	To require controllers to establish unconditionally such procedures, the words "take all reasonable steps" could be deleted from Art 10(3)[8]. *Note: In the Proposed Regulation, controllers are also required to provide an electronic means of access for data subjects if data is processed automatically. However, due to the difficulty of verifying identities electronically, and the potential sensitivity of LEA-held data, an "electronic access" requirement may not be suitable for the Proposed Directive.*
Art 10(4). Controllers must inform data subjects of actions taken in respect of	Controllers must inform data subjects about the follow-up to their request "without undue delay".	(1) Controllers should be required to respond in writing. (This change proposes language set out in Article 12(2) of the Proposed Regulation.)

[8] As proposed in para 365 EDPS Opinion.

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
their requests		(2) Art 10(4) should be rewritten to clearly require controllers to confirm whether or not any action has been taken in respect of their request. Current wording is unclear, and controllers could construe this requirement as only applying if action (i.e., "follow-up") *is* taken. (This change proposes language set out in Article 12(2) of the Proposed Regulation.) (3) In addition to (2) above, if a controller refuses to take action, the controller should be required to inform the data subject of the reason for the refusal, the possibility of lodging a complaint with the supervisory authority, and of seeking judicial remedy. (This change proposes language set out in Article 12(3) of the Proposed Regulation.) *Note: See also chart entries for Art 13 and 14 below.* (4) Controllers should be required to respond to the data subject, whether or not any action has been taken, within a period of 1 month. (This change proposes language set out in Art 12(2) of the Proposed Regulation.)
Art 10(5). Controllers must provide information in respect of requests free of charge, except in certain circumstances	Controllers must provide information free of charge, except if requests are "vexatious, in particular because of their repetitive nature, or the size or volume of the request…".	(1) To make it more difficult for controllers to charge fees for providing information to data subjects, the word "vexatious" in Art 10(5) could be replaced by "manifestly excessive". (This change proposes language set out in Article 12(4) of the Proposed Regulation.) (2) To ensure that data subject rights may be observed regardless of the size or amount of data held, the words "or the size or volume of the request" should be deleted from Art 10(5). (This change proposes language set out in Article 12(4) of the Proposed Regulation.)

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
Art 10. Rights in relation to recipients	The Proposed Regulation would require controllers to communicate any rectification/erasure carried out in accordance with a data subject request to each recipient to whom data have been disclosed, unless this is impossible or would involve disproportionate effort. The Proposed Directive has no equivalent requirement.	Controllers should be required to communicate to each recipient to whom the data have been disclosed any rectification, erasure or change of data, unless this is impossible or would involve disproportionate effort. (This change proposes language set out in Art 13 of the Proposed Regulation.)
Art 11. Information to the data subject	Where personal data are collected, controllers must "take all appropriate measures" to provide the data subject with certain types of information. Art 11 of the Proposed Directive is subject to a significant carve-out (Art 11(4)), that allows Member States to legislate to delay, restrict or omit to provide such information if measures are necessary and proportionate in a democratic society with due regard for the legitimate interests of the person concerned, in order to satisfy one of five prescribed goals (e.g., to protect public security). Additionally, Member States may determine categories of data that are wholly or partly exempt under the above carve-out.	(1) The words "take all appropriate measures" should be removed from Art 11, to unconditionally require controllers to provide such information. (This change proposes language set out in Art 14(1) of the Proposed Regulation.) (2) If data is not collected from the data subject, controllers should be required to inform the data subject from which source the data originates. This requirement should, in the law enforcement context, be subject to the Art 11(4) carve-out. (This change proposes language set out in Art 14(3) of the Proposed Regulation.) (3) The power for Member States to exempt categories of data should be limited, so that controllers are still required to apply the carve-out test of necessity and proportionality on a case-by-case basis[9]. *Note: The wide carve-out means that, in practice, Art 11 will provide much weaker protections for data subjects than its equivalent measure under the Proposed Regulation (Art 14), even if the language of the information to be provided is otherwise exactly the same.*
Art 12. Right of access for the data subject	Data subjects have the right to obtain confirmation from controllers whether or not data relating to them are being processed. If data are being processed, then controllers must provide data subjects with certain types of information about the processing (such as the	(1) Controllers should be required to disclose, so far as possible, the significance and envisaged consequences of processing. (This change proposes language set out in Art 15(1)(h) of the Proposed Regulation.)

[9] As proposed in para 373 EDPS Opinion and in p. 28 Article 29 Working Party Opinion.

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
	categories of data being processed). The data subject also has a right to obtain from the controller a copy of the personal data undergoing processing.	*Note: The Proposed Regulation says that the significance and consequences of the processing of data relating to the data subject information must be provided "at least in the case of measures referred to in Art 20…" The Proposed Directive does not require controllers to provide this information, at least in part because, as set out in this chart below, there is no equivalent provision to Art 20 of the Proposed Regulation (which concerns the right of data subjects not to be subject to certain profiling based measures.)* (2) Where the data subject makes a data subject access request in electronic form, controllers should be required to provide information in electronic form, unless otherwise requested by the data subject. (This change proposes language set out in Art 15(2) of the Proposed Regulation.)
Art 13. Limitations to the right of access	Data subject access rights are subject to a significant carve-out, that allows Member States to legislate to restrict, wholly or partly, data subject access rights to the extent that such restriction is a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned, in order to satisfy one of five prescribed goals (e.g., to protect public security). Additionally, Member States may determine categories of data that are wholly or partly exempt under the above carve-out. If a data subject access right is restricted as a result of such a measure, then the controller must inform the data subject in writing on any refusal or restriction of access, the reason for the refusal, and the possibility of lodging a complaint with a supervisory	(1) Controllers should be required to assess on a case by case basis whether the carve-out can apply, and language should be added to Art 13 requiring that "any restriction must be in compliance with the Charter of Fundamental Rights of the European Union and the Convention for the Protection of Human Rights and Freedoms, and in line with the case law of the European Court of Justice and the European Court of Human Rights"[10]. (2) The power for Member States to exempt categories of data should be limited, so that controllers are still required to apply the carve-out test of necessity and proportionality on a case-by-case basis[11].

[10] As also proposed on p. 29 Article 29 Working Party Opinion.
[11] As proposed in para 373 EDPS Opinion and on p. 28 Article 29 Working Party Opinion.

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
	authority and seeking a judicial remedy (except where the provision of this information would undermine the purpose for which the request was not satisfied). If such information is omitted, to avoid undermining the purpose of the carve-out, then controllers must document the grounds for omitting such factual or legal reasons.	*Note: The wide carve-out means that, in practice, Art 12 will provide much weaker rights for data subjects than its equivalent measure under the Proposed Regulation (Art 15), even if the language of the information to be provided is otherwise exactly the same.*
Art 14 and 45(1)(c). Right for data subject to request supervisory review	Data subjects have a right to request a supervisory authority to review the lawfulness of a controller's processing. Controllers must inform the data subject of the right to request an intervention by the supervisory authority. Where a review is requested, supervisory authorities must inform the data subject that all necessary verifications have taken place, and of the lawfulness of the processing in question.	A power for the relevant supervisory authority to order the controller or processor to comply with data subject requests could be added to this provision, to ensure unambiguously that supervisory authorities are able to enforce the results of their reviews[12].
Art 15. Right to rectification	Data subjects have a right to obtain rectification from the data controller in respect of inaccurate personal data relating to them. Incomplete data may be completed, including by way of a corrective statement. If controllers refuse to rectify such data, they must inform the data subject in writing of the reason for refusal, and on the possibility of lodging a complaint to the supervisory authority and seeking a judicial remedy.	This provision implies that controllers may refuse to comply with data subject rectification requests, but no grounds or conditions for refusal are given. A requirement that any refusal to rectify must satisfy necessity and proportionality tests (along the lines of the carve-out language in Art 11 and Art 13) should be added to Art 15[13].
Art 16(1). Right to erasure	In certain circumstances, data subjects have a right to obtain from the controller erasure of personal data relating to them where processing does not comply with the Art 4(a)-(e), 7 and 8 Proposed Directive (provisions on data processing principles, lawful processing, and processing of special categories of data, respectively). If controllers refuse to erase such data, they must inform the data subject in writing of the reason for refusal, and on the possibility of	This provision implies that controllers may refuse to comply with data subject erasure requests, but no grounds or conditions for refusal are given. A requirement that any refusal to erase must satisfy necessity and proportionality tests (along the lines of the carve-out language in Art 11 and Art 13) should be added to Art 16. (This change is proposed in para 372 EDPS Opinion.)

[12] As proposed in para 379 and Part III 8.a EDPS Opinion

[13] As proposed in para 372 EDPS Opinion.

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
	lodging a complaint to the supervisory authority and seeking a judicial remedy.	*Note: Due to differences between the provisions of the Proposed Directive and Regulation on data processing principles, lawful processing, and processing of special categories of data, the circumstances where data subjects may make a request for erasure are different, and slightly more limited, under the Directive.*
Art 16(3). Right to erasure - "marking"	Instead of erasure, the controller shall "mark" data where (i) their accuracy is contested by the data subject, for a limited period, (ii) the data have to be maintained for purposes of proof, or (iii) the data subject opposes erasure and requests for restriction of use instead.	(1) Art 16(3) should make clear that "marking" data means that data controllers are restricting from processing such data. (This change proposes language set out in Art 17(4) of the Proposed Regulation.) A recital should clarify the meaning of "marked" data, or references to "marking" could simply by replaced by "restrict processing of". *Note: Art 17(4) of the Proposed Regulation requires that the controller "restricts processing" instead of "marking" such data if such circumstances apply. The applicable restrictions are set out in Art 17(5) - 17(6) of the Proposed Regulation -- but no equivalent exists in the Proposed Directive.* (2) Controllers should be required to inform data subjects before "restrictions" or "marks" are lifted and processing resumes. (This change proposes language set out in Art 17(6) of the Proposed Regulation.)
Art 16. Procedure for erasure	The Proposed Regulation sets out procedures for the erasure of data: controllers must implement mechanisms to ensure that time limits established for erasure of data and/or for periodic review of the need for data storage are observed, and controllers must not otherwise process such data. The Proposed Directive has no equivalent requirement.	(1) Controllers should be required to implement mechanisms to ensure that time limits are established for erasure of data and/or that period reviews of the need for data storage are observed. (This change proposes language set out in Art 17(7) of the Proposed Regulation.) (2) Controllers should be required not to otherwise

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
		process erased data. (This change proposes language set out in Art 17(8) of the Proposed Regulation.)
Art 16. Right to be forgotten	The Proposed Regulation provides for a "right to be forgotten", that would require the controller, at the data subject's request, to communicate any rectification/erasure carried out in accordance with a data subject request to each recipient to whom data have been disclosed, unless this is impossible or would involve disproportionate effort. The Proposed Directive has no equivalent requirement.	If requested by the data subject, the controller should be required to "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 such data. Controllers should be responsible for publication of data by third parties, if such publication was authorised by the controller. (This change proposes language set out in Art 17(2) of the Proposed Regulation.)
Other data subject rights found in the Proposed Regulation: the right to data portability and the right to object to processing	The Proposed Regulation sets out rights for data subjects to data portability and to object to processing (see Art 18 and 19 of the Proposed Regulation). The Proposed Directive has no equivalent provisions.	Data subjects should receive a right to object, although it may need to be limited in the law enforcement context (see note below)[14]. *Note: To the extent these rights are viable and applicable in a law enforcement context, such rights should be included in the Proposed Directive. Such rights could be limited by a carve-out similar to the necessity/proportionality carve-out already found in Art 11(4) and 13(1) of the Proposed Directive. However, some elements of such rights -- such as data portability in the context of a criminal investigation, for example -- may not translate effectively across from the Proposed Regulation.*

[14] As proposed in p. 29 Article 29 Working Party Opinion.

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments

Obligations of Controller and Processor

- **Unlike their peers under the Proposed Regulation, controllers are not required to be able to demonstrate compliance with the Proposed Directive.** See Art 18 and 4(f) of the Proposed Directive.

- **Unlike their peers under the Proposed Regulation, controllers are not required to apply data protection by design principles across the whole lifecycle of processing, and are subject to a more limited data protection by default requirement.** See Art 19 of the Proposed Directive.

- **The Proposed Directive is much less prescriptive than the Proposed Regulation when setting out the "required minimum legal terms" that would determine the relationship between processor and controller. In practice, this could make it easier for a controller to use a processor with fewer legal protections for data subjects.** See Art 21 of the Proposed Directive.

- **Controllers are required to document fewer parts of their processing operations, and in less detail, than their peers under the Proposed Regulation. Likewise, they are subject to fewer record-keeping requirements**. See Art 23 and 24 of the Proposed Directive.

- **Unlike their peers under the Proposed Regulation, controllers are never required to communicate data breaches to individuals**. See, by contrast, Art 32 of the Proposed Regulation.

- **Unlike their peers under the Proposed Regulation, controllers are not required to carry out data protection impact assessments**. See, by contrast, Art 33 of the Proposed Regulation.

- **The standard of security safeguards required by the Proposed Directive is less prescriptive than the standard of safeguards required by the Proposed Regulation**. See Art 27 of the Proposed Directive.

- **Controllers are subject to a weaker level of regulatory oversight under the Proposed Directive, and, although required to consult, are not required to seek authorisation from then supervisory authority under any circumstances.** See Art 26 of the Proposed Directive.

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
• **In comparison to the Proposed Regulation, the Proposed Directive provides for less detailed requirements regarding data protection officers, and is less protective of their position**. See Art 30 and 31 of the Proposed Directive.		
Art 18 and 4(f). Responsibilities of the controller	Controllers must adopt policies and implement appropriate measures to ensure processing is performed in compliance with the Proposed Directive. Specifically, controllers are required to comply with Art 23, 26, 27 and 30 of the Proposed Directive. As discussed further below, this list leaves out obligations set out in the Proposed Regulation, such as the requirement for controllers to perform data protection assessments. Controllers must also implement verification mechanisms, and, if proportionate, such verification must be performed by independent internal or external auditors.	Controllers could be required to "demonstrate" that their processing is in compliance with the Proposed Directive (in addition to their obligation to ensure their own compliance). (This change proposes language set out in Art 22(1) of the Proposed Regulation.)
Art 19(1). Data protection by design	Controllers shall implement appropriate technical/organisational measures to ensure compliance with the Proposed Directive and to protect the rights of the data subject (privacy by design).	The language "both at the time of determination of the means for processing and at the time of processing itself" could be added to Art 19(1), to make clear that controllers must ensure appropriate technical/organisational measures both before, and during, processing. (This change proposes language set out in Art 23(1) of the Proposed Regulation.)
Art 19(2). Data protection by default	Controllers shall implement mechanisms for ensuring that, by default, only data that are necessary for the purposes of processing are processed.	(1) Controllers should also be required to implement mechanisms to ensure that by default data are not collected or retained beyond the minimum necessary for the purpose of processing (both in terms of amount of data and time of storage). (This change proposes language set out in Art 23(2) of the Proposed Regulation.) (2) This requirement could be clarified, to make clear that mechanisms should by default ensure that data are not made available to an indefinite number of individuals. (This change proposes language set out in Art 23(2) of the Proposed Regulation.)

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
Art 21(2). Processor -- legal basis for processor relationship	Processors may only process under a legal act that binds the processor to the controller and that stipulates that the processor will only act on instructions from the controller, in particular, where the transfer of data is prohibited.	This provision could be made more prescriptive, by requiring the legal act that binds the processor to state that: (i) only staff committed under statutory obligation of confidentiality should be used for processing; (ii) all security measures under Art 27 of the Proposed Directive (security of processing) must be observed; (iii) another processor may only be enlisted with permission of the controller; (iv) if possible, the controller and processor should be required to create necessary technical and organisational elements required for fulfilment of data subject requests; (v) the processor will aid the controller in compliance with Art 27 - 29 of the Proposed Directive (on data security); (vi) the processor must hand over all results of processing to the controller after processing, and will not otherwise process the data; and (vii) the processor must make available to the controller and supervisory authority all information necessary to comply with Art 25 of the Proposed Directive. (This change proposes language set out in Art 26(2) of the Proposed Regulation.)
Art 23. Documentation	Controllers and processors must maintain documentation of all processing systems and procedures under their responsibility. Documentation must contain prescribed information (e.g., the purposes of processing). In the case of a data transfer, documentation must state the identity of the international organisation or third country that received the data. Controller and processor must make documentation available to the supervisory authority on request.	(1) Documentation should be required to include further categories of prescribed information, including: (i) a description of the categories of data subjects and categories of personal data relating to them; (ii) a general indication of the time limits for erasure of the different categories of data (if applicable); (iii) a description of the mechanisms used to ensure and verify the effectiveness of the measures required of controllers under Art 18 of the Proposed Directive; and (iv) the name and contact details of the data protection officer. (This change proposes language set out in Art 28(2) of

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
		the Proposed Regulation.) *Note: In the list above, items (ii) re data retention periods and (iv) re contact details of the data protection officer are particularly important and must be included in the documentation requirement.* (2) Documentation to be kept in case of a data transfer could include more details of the grounds on which such a transfer is made and, if appropriate, a substantive explanation[15].
Art 24. Keeping of records	Member States must ensure that records are kept of certain prescribed processing operations. The records shall be used solely for the purposes of verification of the lawfulness of processing and for ensuring data integrity/security.	This provision could also prescribe record-keeping of the identity of every recipient of the data. This provision could assure access to these records for the supervisory authority.[16]
Communication of data breach to data subject	The Proposed Regulation requires that, where a data breach is likely to adversely affect the protection of data or the privacy of the data subject, controllers must (after notifying the supervisory authority) communicate the breach to the data subject without undue delay. The Proposed Directive has no equivalent provision.	*Note: We suggest that, to the extent this obligation is viable and applicable in a law enforcement context, such obligation should be included in the Proposed Directive.*
Data protection impact assessments	The Proposed Regulation requires that, where processing operations present specific risks to the rights and freedoms of data subjects, controllers carry out a data protection impact assessment. Details of the nature of assessments are described. The Proposed Directive has no equivalent provision.	Controllers could be required to carry out data protection impact assessments, given the sensitive nature of data processing in the law enforcement context.[17] *Note: Even in cases where data protection impact assessments have already taken place during a legislative process, data protection impact assessments should be required as systems, processes and technologies change over time.*
Art 26. Prior consultation	Controllers are, in certain cases, required to consult with the supervisory authority before establishing a new filing system for	Controllers should be required to seek prior consultation whenever a new processing operation

[15] Also proposed in para 395 EDPS Opinion.

[16] Also proposed in para 396 EDPS Opinion.

[17] Also proposed in para 385 and 398 EDPS Opinion and on p. 29 of the Article 29 Working Party Opinion

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
	personal data. Member States may empower supervisory authorities to compile a list of processing operations that would require such prior consultation.	would be introduced into a filing system. (This change proposes language set out in Art 34 of the Proposed Regulation.)
Art 27. Security of processing	Controllers/processors are required to implement appropriate technical and organisational measures to ensure security appropriate to the risks, and with regard to the state of the art and the costs of implementation.	Controllers/processors should be subject to a higher standard of security requirements; for example, requiring them to take measures to guard against accidental loss or damage[18].
Art 30. Data protection officer	Controllers (or processors if applicable) must designate a data protection officer (DPO). The DPO must be designated on the basis of professional qualities and expert knowledge of data protection law and practice, and ability to fulfil tasks set out in Art 32 of the Proposed Directive. DPOs may be designated for multiple entities.	This provision could be more prescriptive: (i) to require a necessary level of expert knowledge in relation to the type of processing contemplated; (ii) to require that the DPO's other professional commitments are compatible with the person's tasks and duties as a DPO and do not result in a conflict of interests; (iii) to require designation of a DPO for at least 2 years, and to protect the DPO from dismissal; (iv) to give data subjects the right to contact the DPO; and (v) to specify the controller or processor shall communicate the name of the DPO to the supervisory authority and to the public. (This change proposes language set out in Art 35 of the Proposed Regulation.)
Art 31. Position of data protection officer	Controllers (or processors if applicable) must ensure that the DPO is properly and in a timely manner involved in all issues that relate to the protection of personal data. Controllers (or processors if applicable) must ensure that the DPO is provided with the means to perform their duties effectively and independently, and does not receive any instruction regarding such.	(1) Controllers (or processors if applicable) should be required to ensure that the DPO reports directly to senior management. (This change proposes language set out in Art 36(2) of the Proposed Regulation.) (2) Controllers (or processors if applicable) should be required to support the DPO with staff, premises, equipment, and any other necessary resources. (This change proposes language set out in Art 36(3) of the Proposed Regulation.)
Miscellaneous		

[18] Also proposed in p. 29 Article 29 Working Party

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
• **Transfer rules do not apparently prevent transfers of data to non-"competent authority" recipients**. **In some cases, controllers may be able to "self-assess" whether or not to send data to a third country, whether or not that country has been identified as adequate. Derogations from the transfer rules are very broad. Controllers are not required to inform data subjects of transfers to other Member States**. See Art 33, 35, and 36 of the Proposed Directive. • **Supervisory authorities have fewer, and more ambiguous, powers, in comparison to their peers under the Proposed Regulation**. See Art 46 of the Proposed Directive. • **Requirements to ensure mutual assistance and consistency in relation to cooperation between supervisory authorities are ambiguous, and less comprehensive, than similar provisions under the Proposed Regulation**. See Art 48 of the Proposed Directive.		
Art 33. Conditions for international data transfers	Transfers may only take place if (i) the transfer is necessary for the prevention, investigation, detection or prosecution of crime or the execution of criminal penalties, and (ii) further conditions set down in Chapter V of the Proposed Directive are complied with.	In accordance with existing legal instruments, Art 33 could specify that transfers may only be made to controllers in a third country or international organisation that are competent authorities for law enforcement purposes[19].
Art 35(1)(b). Transfers by way of appropriate safeguards	Where no adequacy decision has been taken in respect of a third country, the controller may transfer data to such country provided either that (i) appropriate safeguards are adduced in a legally binding instrument or (ii) they have assessed all the circumstances surrounding the transfer and concluded that appropriate safeguards exist. Such an assessment must be made by duly authorised staff, and all such transfers must be documented (and documents must be made available to the supervisory authority on request).	(1) Controllers should be required to obtain an assessment of whether safeguards are adequate from the supervisory authority, rather than making such an assessment themselves. (This change proposes language set out in Art 42(5) of the Proposed Regulation.) (2) If the above improvement is not feasible, then controllers could be required to document safeguards taken if a self-assessment is the basis for transfer[20]. *Note: There is also lack of clarity between this Article and Art 34 (6) which refers to prohibition by the Commission to data transfers to a certain third country*

[19] Also proposed in para 409-410 EDPS and in p.30 and p.32 Article 29 Working Party Opinion
[20] Also proposed in p. 30 Article 29 Working Party Opinion

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
		or international organisation. There is need for clarification of these two provisions.
Art 36. Derogations from transfer rules	Transfers of data to third countries or international organisations may take place only on certain conditions, which are prescribed. One such condition is that the transfer is "necessary".	(1) Such "conditions" for transfer are open to wide interpretation, and so further language could be inserted to Art 36 to make clear that each such "condition" should be interpreted restrictively[21]. (2) Controllers could be required to document any use of the derogations in Art 36, and any such documentation could be required to be available to the relevant supervisory authority on request[22].
Art 46. Powers of the supervisory authority	Supervisory authorities are endowed with investigative powers, powers of intervention, and powers to engage in legal proceedings. Examples of each type of power are given.	(1) Each "example" of the three types of power listed in Art 46 could be converted into "core" powers for supervisory authorities, that Member States are required to legislate for in specific terms.[23] (2) Supervisory authorities could receive more powers under this provision, including: (i) power to notify controllers/processors of alleged breaches, and to order the controller/processor to remedy the breach in a specific manner; (ii) power to order the controller/processor to comply with the data subject requests; (iii) power to order the controller/processor to provide information relevant for performance of their duties; (iv) power to ensure compliance with prior consultations (and authorisations, if that revision is made) under Art 26 of the Proposed Directive; (v) power to warn/admonish controllers/processors;

[21] Also proposed in p. 31 Article 29 Working Party Opinion
[22] Also proposed in p. 31 Article 29 Working Party Opinion

[23] Also proposed in 430 EDPS Opinion.)

Article of the Proposed Directive and issue area	Existing requirement of the Proposed Directive	Improvements needed and comments
		(vi) power to order rectification, erasure or destruction of data if such data have been processed in breach of the Proposed Directive, and the notification of such action to third party recipients; (vii) power to impose a temporary or permanent ban on processing; (viii) power to suspend data flows to recipients in third countries or to international organisations; (ix) power to issue opinions related to issues of data protection related to the Proposed Directive; (x) power to inform national legislature and other political institutions, as well as the public, about data protection issues. (This change proposes language set out in Art 53(1) of the Proposed Regulation.) *Note: As noted also in p. 31 Article 29 Working Party Opinion, the powers awarded to national supervisory authorities are both sparse and vague, and in particular there is lack of clear power for these to enter premises of controllers when necessary*.
Art 48. Mutual assistance between supervisory authorities	The Proposed Regulation sets out a number of rules that require supervisory authorities to cooperate with one another on standardised and mandatory terms. The Proposed Directive contains much more limited provisions for such cooperation.	A stronger mechanism of mandatory cooperation between supervisory authorities could be included in the Proposed Directive, and specific time limits for cooperative actions could be set out in order to make such cooperation mandatory. (This change proposes language set out in Art 55(2)-(7) of the Proposed Regulation.)