EDRi's Position on the Proposal for a Directive of the European Parliament and of the Council 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

(Directive on Data Protection in Law-Enforcement)

COM(2012)10 final

European Digital Rights
Rue Belliard 20, 1040 Brussels
Tel:+**32 2 274 25 70**
E-Mail: brussels@edri.org, http://www.edri.org

Table of Contents

European Digital Rights
Rue Belliard 20, 1040 Brussels
Tel:+**32 2 274 25 70**
E-Mail: brussels@edri.org, http://www.edri.org

GENERAL ASSESSMENT OF THE PROPOSED DIRECTIVE

The current situation for the data protection in the law-enforcement sector is unsatisfactory. Even though the proposed Directive takes some steps to ameliorate certain aspects of the current framework and would also cover domestic processing, EDRi points out that the proposed rules are too weak in many aspects:

- data subject rights are unduly restricted;
- obligations on controllers are too limited;
- data protection authorities do not have all necessary powers;
- specific rules on the relation with controllers in the private sector are missing;
- safeguards for data transfers to third countries are insufficient;
- the transition periods for adapting current legislation are too long, prolonging the current, unsatisfactory, situation.

The current Framework Decision 2008/977/JHA only sets out weak rules for transfers between competent authorities in the Member States and excludes domestic processing. Additionally, there are a number of specialised instruments regulating specific exchanges. This patchwork is non-transparent and provides insufficient protection. With the entry into force of the Lisbon Treaty, Article 16 of the Treaty offered the possibility to have horizontal rules regulating data protection across all sectors, including law-enforcement, which could help overcome the current fragmentation. However, the Commission decided to propose two separate instruments: the General Data Protection Regulation for the private and most of the public sector, and a Directive for the law-enforcement sector. The choice of a Directive as legal instrument for the law enforcement sector seems to be a reflection of political realities in the Council, where Member States are reluctant regarding greater harmonisation.

Nonetheless, a Directive still offers the potential to improve the status quo by setting out rules not only for transfers, but also for domestic processing, and by overcoming the current patchwork. However, the proposed Directive falls far short of these aims and suffers from many problems.

While EDRi welcomes that the scope of the proposed Directive shall also cover domestic processing, this improvement is mostly formal: in many instances, the rules in the proposed Directive are less precise and offer less protection to individuals than those in the proposed Regulation. So while there would be comparable rules throughout Europe, they would be weak.

Examples for this are data subject rights, the obligations on controllers, and the competences of supervisory authorities. Compared to the Regulation, less information will be given to data subjects, controllers do not have explicit time limits for replying to access requests, the rules on profiling are too weak, and there are no specific rules on the processing of children's data. Controllers also do not have to demonstrate compliance with data protection rules, as they obliged to under the Regulation. Finally, the competences of supervisory authorities are weaker than under the Regulation. Each of these aspects is further developed in separate position papers.

Given that the Directive deals with processing of very sensitive data and can have grave impacts on data subjects' fundamental rights, having such weak protection rules is unacceptable. Of course, there are situations in which (temporary) limitations can be justified, but the core of the rules must

be strong and consistent with the Regulation, the EU Charter of Fundamental Rights and the European Convention on Human Rights. There appears to be a real danger that the Directive's rules with regard to domestic processing would be weaker than current rules in the countries which have the strictest standards. As a result the Directive could lower data protection standards in certain Member States, which cannot be accepted. The European Commission should provide a detailed assessment of its proposed harmonisation through the Directive to guarantee that the Directive does not result in lowering privacy and data protection safeguards.

Failing to have strict standards that are equivalent to the proposed Regulation would not only undermine the protection of the fundamental rights to data protection and private life, but would also lead to additional inconsistencies. There are notable differences between how Member States define the activities of their authorities, for example in matters such as customs, immigration, and environmental affairs. Sometimes these are labelled as law-enforcement, and sometimes as administrative proceedings. This can lead to situations in which the same activity would be covered by the (national legislation implementing the) Directive in one Member State, and by the Regulation in another.

Not only between Member States, but also between sectors, problems remain: one of the most important developments in the law-enforcement sector in the recent past is its increasing reliance on data held by private actors, be it traffic data from telecoms providers, data stored by web hosting providers, or any other data. The rules on how to access such data need to be clear and strict. Yet, such rules are mostly absent from both the Regulation and the Directive. Similarly strong rules are needed for transfers from law-enforcement authorities to other recipients.

Increased transfers to third countries are another important development. Here, the rules proposed in the Directive are not strict enough – for example, they do not specify that data should only be transferred to competent authorities in third countries, opening a loophole for transfers to private controllers – and offer excessive room for derogations.

Even if all these problems were fixed, the Directive would still not comprehensively deal with the current patchwork of data protection rules in law-enforcement matters: Article 59 states that existing instruments in the area should remain unaffected by the Directive, while Article 61 obliges the Commission to evaluate these prior acts within three years of the entry into force of the proposed Directive, and where necessary, make proposals for amendments. International agreements in this area are supposed to be amended, where necessary, within five years of entry into force of the Directive. These grandfathering clauses significantly delay any possible improvements of data protection framework. In both cases, these periods should be shorter.

As it currently stands, the proposed Directive is mostly a missed opportunity. EDRi provides further analysis of the Directive's shortcomings and proposes concrete amendments to address them in the position papers contained in this collection.

PROFILING

The use of profiling of individuals is increasing, also in the law-enforcement sector. Given that profiling can affect large numbers of data subjects, most of whom will have done nothing unlawful, and because it can be very invasive, it should be tightly regulated.

(1) OUR ANALYSIS:
Profiling is fraught with many problems. The first is what statisticians call the "base rate fallacy". It refers to the mathematically unavoidable fact that if you are looking for very rare instances in a very large data set, then no matter how well you design your algorithm, you will always end up with either excessive numbers of "false positives" (cases or individuals that are wrongly identified as belonging to the rare class), or "false negatives" (cases or individuals that do fall within in the rare, looked-for category, but are not identified as such), or both. This limitation is inherent in profiling and should be remembered every time it is used.

The second problem is that profiling tends to reproduce societal discrimination of "out-groups", even if characteristics such as ethnic or racial origin are not overtly part of the profiling algorithm. Discrimination can still creep in and perpetuate existing discrimination in the guise of scientifically defensible profiles. In this regard, it should be noted that under international human rights law, "unintentional" discrimination is outlawed just as well.

The third problem is related to technological advances: with data mining and analysis techniques becoming more and more sophisticated, it can become difficult to understand the logic behind the profiling – even for the authorities using it. This reinforces the two first problems mentioned above and also makes decisions based on profiles harder to challenge, since even the authorities making the decision might often not be able to supply a better explanation than "because the computer said so".

These problems make it abundantly clear that the use of profiling should be tightly regulated. Article 9 of the proposed Directive sets out rules on profiling and contains some protection against measures based on profiling. However, unlike their peers under the proposed Regulation, individuals have no right not to be subject to such measures. What also needs to be noted is that a clear definition of "profiling" itself is missing – the term is defined neither in Article 9, nor in Article 4.

It is not clear from the Commission proposal how the main criterion for recognising an activity as profiling, namely that it "produce[s] an adverse legal effect for the data subject or significantly affect[s] them" should be interpreted. In our opinion, this formulation is too narrow and could lead to a situation where the prohibition of using measures based on profiling and automated processing, which was adopted as a general principle, will be unreasonably diluted. This is another reason for having a clear definition.

While the starting point of prohibiting profiling as a general rule and then allowing certain exceptions is the right one, we are also concerned about the scope of exceptions. Under the

Commission proposal, profiling would be allowed if it is "authorised by a law which also lays down measures to safeguard the data subject's legitimate interests". This formulation is too general and does not guarantee an adequate level of protection of the rights of the data subject. In every case, profiling should be accompanied by specific safeguards. This applies especially to the use of sensitive data (such as data on race or ethnic origin, political opinions and religious beliefs). The proposed Directive simply says that profiling shall not be based "solely" on such characteristics. This is too weak; similarly, it does not offer adequate protection against discrimination via profiling and does not guarantee the data subject's right to information on the logic behind the profile.

(2) OUR RECOMMENDATIONS:

- The definition of profiling should be brought in line with the Council of Europe Recommendation CM/Rec(2010)13. Such an explicit definition should be included in Article 4.
- The proposed Directive should require that laws allowing profiling shall be subject to a strict test of necessity and proportionality, which would have to demonstrate that profiling is necessary in a given situation and does not affect the vital interests of a person concerned.
- It should be clarified that profiling shall not be based on or generate any of the special categories of personal data specified in Article 8 of the proposed Directive.
- Profiling that leads – intentionally or unintentionally – to discrimination based on such special categories should be completely prohibited.
- When informing data subjects about the profiling measure, they should also be given information on the logic behind the profiling. This mirrors recommendations EDRi made to the provisions on profiling in the proposed General Data Protection Regulation.
- To strengthen the ability of individuals to enforce the prohibition of profiling, Article 9 should be revised to give individuals a right not to be subject to such measures.

DATA SUBJECT RIGHTS

EDRi broadly welcomes the provisions in the Proposed Directive, which strengthen and clarify the rights of the data subject through measures aiming for greater accountability of the controller, in particular with respect to data subject's right to information and right of access. There is, however, a number of provisions that should be amended in order to avoid any excessive restrictions on data subjects' rights. EDRi believes that the level of protection afforded by the proposed Directive should be comparable to the level of protection foreseen by the proposed General Data Protection Regulation,

Modalities for exercising data subjects' rights (Article 10)

(1) Our analysis:
Exercising one's data protection rights is made easier under the proposed Regulation than under the proposed Directive. While the proposed Regulation *requires* controllers to have policies on data processing and to set up procedures for providing information on processing to data subjects and for exercising their rights, the proposed Directive only prescribes that the controller *takes all reasonable steps* to have such policies and procedures. This wording aims at limiting the responsibility of the controllers for not establishing procedures and policies that in practice are essential for data subjects to execute their rights. In consequence, the wording of Article 10(1) and 10(3) may lead to the rights of data subjects being conditional upon the assessment (made by the controller) whether it is reasonable or not to have necessary policies and to establish necessary procedures. EDRi believes that these requirements should be unconditional as they are the key to an effective exercise of data subjects' rights.

Moreover, the provision on the controller's reply to a data subject's request (Article 10(4)) should provide for exact obligations of the controller and a determined deadline for the reply, akin to the corresponding Article 12 of the proposed Regulation. If a data subject is left without a reply for months, then their rights exercised through a request become meaningless.

Another issue that needs to be addressed is the possibility for data controllers not to take the action requested by the data subject if a request is "vexatious", or to charge fees for taking requested actions (Article 10(5)). While the objective of this provision is justified as it seeks to prevent the abuse of rights, its wording has to be chosen carefully in order not to prejudice the legitimate exercise of data subject rights. This provision can be contrasted with its counterpart in Article 12(4) of the proposed Regulation, which only allows charging fees for "manifestly excessive" requests. In EDRi's view, there is no reason why there should be a lower standard under the proposed Directive.

The above changes are necessary in order to *truly* allow data subjects to exercise their rights foreseen by the Directive.

(2) Our recommendations:

- The words "take all reasonable steps" should be deleted from Article 10(1) and Article 10(3).
- The controller should be obliged to reply to a data subject's request in writing and sent within one month from the reception of the data subject's request. The controller should also be required to inform the data subject whether or not any action has been taken following a data subject's request (under the current wording of Article 10(4), it may appear that controllers should only reply if action is taken).
- The wording of Article 10(5) should be brought in line with that of its peer Article 12(4) of the proposed Regulation: controllers should only be allowed to charge fees for taking the action requested by the data subject, or not to take the action requested, if requests are "manifestly excessive", and not just "vexatious". Moreover, the criterion of "the size of volume of the request" (based on which controllers may charge fees or not take the action requested at all) should be deleted, so that data subjects' rights are observed regardless of the size or amount of data held by the controller.

Duty to provide information to data subjects and right of access (Articles 11-14)

(1) Our analysis:

In general, according to the proposed Directive, controllers are under a duty to provide information to data subjects and to allow them access to their data. Safeguarding these important principles deserves a merit. But comparing to the proposed Regulation, controllers may be less transparent and less responsive to requests, and slower to respond. In addition, the proposed Directive provides for very broad exemptions, which may render the fundamental right to data protection meaningless.

According to Articles 11 and 13, controllers' duty to provide information to data subjects and data subjects' access rights are subject to a significant carve-out that allows Member States to legislate to restrict these 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.

Delaying, restricting or omitting the provision of the information to the data subject as well as the total or partial restriction of the data subject's right of access are allowed, for example, in order to protect public or national security. EDRi is concerned about the difficulty in distinguishing between these two categories, as well as the possibility of their broad interpretation. It should also be noted this wide carve-out means that, in practice, Article 12 will provide much weaker rights for data subjects than its equivalent measure under the proposed Regulation (Article 15), even if the language of the information to be provided is otherwise exactly the same.

(2) Our recommendations:

- In principle EDRi welcomes an explicit reference to the test of necessity and proportionality. However, as it could be observed for example in the debate about mandatory telecommunications data retention, this concept remains susceptible to different

interpretations depending on the legal culture and current political context. In this context EDRi recommends that Member States should be obliged to notify their proposals for legislative measures relying on this particular exemption to their data protection authority for consultation. Language should be added to Article 11 and 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 Court of Justice of the European Union and the European Court of Human Rights". As an alternative, such language could be introduced in a recital, akin to Recital 59 of the proposed Regulation.

- The power of Member States to completely exempt certain categories of data from the right of access by the means of legislative measures (Article 13(2)) should be removed. The possible restrictions in Article 13(1) are sufficient.
- Similar considerations apply to Article 11(5).
- The words "take all appropriate measures" should also be removed from Art 11(1), to unconditionally require controllers to provide the data subject with the types of information mentioned in this article.
- In more general terms EDRi recommends that the amount and scope of exemptions provided for in the Proposed Directive should be reconsidered and limited in order to achieve similar standards of the protection of the data subject's rights. Every single exemption has to be duly justified, while blanket and broad exemptions can not be accepted. Limitations of the rights of data subjects must be an exception to the general rule, and cannot become the rule itself.

Rights to erasure and rectification (Articles 15-16)

(1) Our analysis:

In the language of the proposed Directive, the rights to erasure and rectification of data are far more limited and more unclear than they are under the proposed Regulation. Article 15, dealing with the right to rectification, states that controllers may refuse to comply with data subject rectification request, but it does not give any grounds or conditions for that. According to Article 16, which deals with the right to erasure, controllers may refuse to comply with data subject erasure requests – but again, no grounds or conditions for refusal are formulated.

The proposed Regulation provides for a "right to be forgotten" that would require the controller to communicate any rectification/erasure carried out in accordance with a data subject's request to each recipient to whom data have been disclosed, unless this is impossible or would involve disproportionate effort (Article 17(2) of the draft Regulation). The provision serves to protect data subjects' rights in case their data are transferred to a third party. The Proposed Directive has no equivalent requirement. EDRi believes that a similar obligation should also apply in the law enforcement area, where it is crucial that data are not processed unlawfully. At the least, any rectification or erasure carried out by a controller should be communicated to all the data recipients, as is the case under Article 13 of the proposed Regulation. This would guarantee the accuracy of data.

Under Article 16(3), the controller has to "mark" the data instead of erasing them in specific, enumerated situations. However, what such "marking" actually means is not defined. In the corresponding Article 17(4) of the draft Regulation, the term "restricting processing" is used, which means that data can only be stored, and processed for a limited in very limited cases (e.g. for purposes of proof or for the protection of the rights of another natural or legal person). Moreover, under the draft Regulation data subjects are informed before the restrictions are lifted and processing resumes (Article 17(6)). Similar provisions should be introduced in the draft Directive.

(2) Our recommendations:

- EDRi recommends that the conditions for refusal to rectify or erase data should be clarified. Controllers should not be able to deny rectification requests that are factually correct; similarly, they should not be able to deny erasure of unlawfully processed data.
- An equivalent of Article 13 of the draft Regulation should be introduced, which would require controllers to communicate any rectification carried out in accordance with a data subject's request to each recipient to whom data have been disclosed.
- Article 16 (with regard to "marking" data instead of erasing them) should be brought in line with Article 17(5)-(6) of the draft Regulation – "marking" should be clearly defined or replaced by "restricting processing". Also, data subjects should be informed before such marks are lifted and normal processing resumes.

OBLIGATIONS OF CONTROLLERS

The obligations to which controllers are subject must at all times be clear and as detailed as possible. This is one of the keys to good protection of personal data. Having controllers be subject to clear rules will clarify the responsibilities of controllers. Clear rules will also benefit supervisory authorities when investigating data protection breaches, especially where these rules ensure the availability of adequate documentation regarding the processing of personal data.

(1) OUR ANALYSIS

The rules on obligations of controllers under the proposed Directive differ from those under the proposed Regulation in several important aspects. The obligations imposed by the proposed Directive are far less detailed and less strict. Specific measures and procedures introduced in the proposed Regulation are missing in the proposed Directive. For instance, controllers under the Directive do not need to carry out data protection impact assessments or lay down obligations of processors in writing. The obligation to adhere to the principles of privacy by design and default is watered down, and the documentation requirements are far more limited than those laid down in the proposed Regulation. Additionally, controllers are subject to a lower level of regulatory control, and the controller-processor relationships are regulated in less detail and with fewer safeguards for individuals.

This is both alarming and surprising, given the fact that controllers under the scope of the proposed Directive – such as police authorities and public prosecutors – by their very nature deal with personal data that are sensitive and use them to take decisions that can seriously affect data subjects. Therefore the rules of the proposed Directive should rather be stricter than under the proposed Regulation.

Only in one case, controllers under the Directive face more fine-grained requirements: they are supposed to keep detailed records of their processing operations. A police database would for example have to log which data were combined for which purpose at which time. If possible, such a controller must also log which officer consulted which records. The table below lists the most important differences between the controller obligations listed in the Regulation versus those of the Directive.

Regulation	Directive	Difference
Article 22 (1)	Article 18(1)	Under the Directive, controllers do not need to be able to "demonstrate" compliance with data protection rules.
Article 22 (2) (b)	-	Under the draft Directive, controllers are not obliged to conduct data protection impact assessments.
Article 22 (3)	Article 18 (3)	Article 18(3) of the draft Directive does not contain a reference to paragraph 2(which would add clarification).
Article 23 (2)	Article 19 (2)	While the Regulation obliges controllers to implement data protection by design both at the design stage and in the actual processing, the Directive does not make this distinction. The requirements for data protection by default are less specific: there are no references to maximum storage periods of data or their

		publication.
Article 26 (1)	Article 21 (1)	The Directive is less specific as regards technical measures to be implemented by processors.
Article 26 (2) (a) to (h)	Article 21 (2)	There is no list of specific requirements for the controller-processor relationship in the Directive.
Article 26 (3)	-	The requirement to lay down processor's obligations in writing does not exist.
Article 28 (2)	Article 23 (2)	The scope of what needs to be documented is different: under the Regulation, such documentation has to be maintained for all "processing operations", while under the Directive "processing systems and procedures" need to be documented. The list of items to include in the documentation is shorter as well: • no contact information for the data protection officer; • no description of categories of data subjects and the categories of personal data relating to them; • no documentation of safeguards for 3rd country transfers; • no mention of retention periods; • no description of accountability mechanisms.
-	Article 24	This Article obliges controllers to keep detailed logfiles on their systems, but only "as far as possible", which is why it hardly qualifies as an obligation
Article 29 (1)	Article 25 (1)	The rules on cooperation with supervisory authorities are more vague, as their powers are described less clearly under the Directive.
Article 29 (2)	Article 29 (2)	In both cases, controllers need to reply to the supervisory authority within a "reasonable period", however only under the Regulation this period is fixed by the supervisory authority.
Article 33	-	No rules on data protection impact assessments.

(2) OUR RECOMMENDATIONS

Simply put, we recommend that the controller obligations in the proposed Directive be brought in line with those in the proposed Regulation (and the amendments we proposed there). More specifically we suggest the following changes:

- Article 18(1): include the requirement of being able to "demonstrate" compliance;
- Article 19: align with the proposed Regulation and explain that both technical and organisational measures should be used to implement data protection by design and by default, add a reference to data protection impact assessments;
- Article 21(2): include the list of requirements from Article 26(2) of the proposed Regulation;
- Article 21(2a): add a new paragraph, equivalent to Article 26(3) of the proposed Regulation,

requiring written documentation of controllers' instructions and processors' obligations.

- Article 23(1): align with the documentation requirements in Article 28(2) of the proposed Regulation and include a requirement for a substantive explanation for 3rd country transfers based on appropriate safeguards or derogations;
- Article 24: clarify that these records shall be made available to the supervisory authority on request;
- Article 25: align with Article 29 of the proposed Regulation by specifying that the "reasonable period" is to be specified by the supervisory authority;
- Article 26(1): require prior authorisation also in cases where measures based on profiling are to be carried out and when a data protection impact assessment has been carried out;
- New Article 29a: introduce rules on data protection impact assessment, based on Article 33 of the proposed Regulation.

TRANSFERS TO THIRD COUNTRIES

Transfer of data to third countries is a sensitive subject. The Directive is trying to serve two goals that appear to be in conflict: protecting personal data and facilitating the flow of personal data, including in certain cases to third countries outside the EU that may not provide for adequate protection of personal data.

(1) OUR ANALYSIS:

Chapter V sets out general principles for the transfer of personal data to third countries or international organisations in the field of police and judicial cooperation in criminal matters, including onward transfers. According to the basic principle expressed in Article 33, transfers to third countries may take place only if it is "necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" and when the controller and processor comply with the conditions specified in the Directive. At the same time, the provisions of Chapter V, in particular Article 35(1)(b) and Article 36, provide for very broad exceptions to this general rule, which may lead to systemic abuses and avoidance of the basic principles expressed in Article 33.

According to **Recital 45** and **Article 33**, Member States should ensure that a transfer to a third country only takes place if it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Furthermore, the controller in the third country or international organisation has to be a "competent authority" in the meaning adopted by the Directive. It should be clarified that transfers may only occur to **public** authorities competent for law enforcement purposes in third countries and not other recipients. This has also been suggested by the European Data Protection Supervisor (EDPS) and the Article 29 Working Party. Similar changes should also be introduced in all other Articles allowing transfers to third countries and international organisations.

There is currently no specific provision concerning the issue of **onward transfers**. Therefore, we propose to add a new paragraph in **Article 33** to cover this matter; our proposed **recital 45a** provides additional explanation. In our opinion, onward transfers should only be allowed if they are necessary for the same specific reason that justified the original transfer, for example when they are necessary for investigating the same case that prompted the original transfer, but not for general law-enforcement purposes. Additionally, the competent authority that carried out the original transfer should authorise the onward transfer.

Article 34 regulates the issue of **transfers with an adequacy decision.** By analogy to the amendments that we suggested to the General Data Protection Regulation, EDRi recommends that the **European Data Protection Board** (EPDB) should be consulted before issuing (non-)adequacy decisions.

Article 35 regulates the issue of **transfers by way of appropriate safeguards.** In our opinion, self-assessments of safeguards with respect to data protection by the controller or processor cannot provide a basis for such transfers, especially given that their own interests might influence their judgement as to whether the safeguards are appropriate. Such transfers should always be based on a legally binding instrument. Therefore, we support the EDPS in his opinion that Article 35(1)(b)

should be deleted.

Derogations from the preceding provisions are regulated in **Article 36**. According to this provision, in the absence of an adequacy decision taken pursuant to Article 34 or of appropriate safeguards adduced pursuant to Article 35, transfers of data to third countries or international organisations may still take place only if certain conditions are fulfilled. However, these conditions could be open to wide interpretation and in effect, controllers might often rely on the derogations, even if a transfer of personal data is not strictly necessary. We therefore think that the use of such derogations should be limited to the minimum and that additional safeguards should be put in place. Moreover, all transfers should be properly documented.

(2) OUR RECCOMMENDATIONS

- Specify that transfers should only occur to *public* authorities competent for law enforcement purposes;
- Introduce specific rules restricting onward transfers, i.e. they should only be allowed if they are necessary for the same specific reason that justified the original transfer, and should be subject to authorisation by the authority that carried out the original transfer;
- The Commission should consult the EDPB before an adequacy decisions is issued;
- Remove the possibility of self-assessment by the controller or processor as to whether appropriate safeguards exist (delete Art. 35(1)(b));
- Restrict the use of derogations by introducing a requirement that any transfers under Article 36 have to be subject to a prior authorisation by the supervisory authority and that they have to be duly documented.

COMPETENCES OF SUPERVISORY AUTHORITIES

Enforcement powers for supervisory authorities are the teeth of data protection. Given that the processing of personal data in the law-enforcement sector often has grave consequences for individuals, enforcement rules need to be strong.

(1) OUR ANALYSIS

The rules on supervisory authorities are modelled on those in the proposed General Data Protection Regulation. This makes sense, as it is highly likely that the same authorities will be designated as supervisory authorities under both texts. In many cases, the rules are identical or highly similar, for example as regards the independence of supervisory authorities. Yet, there are some important differences, most notably as regards their powers.

While under the proposed Regulation, contains a long list of specific powers of supervisory authorities (see Article 53 of the proposed Regulation), the provisions of the proposed Directive are less clear: **Article 46** mentions that supervisory authorities should have investigative powers and powers of intervention (each accompanied by a list of examples), as well as the power to engage in legal proceedings. While these rules can potentially be strong – national legislators could easily copy & paste the rules from the proposed Regulation with some editorial changes – they also offer Member States the possibility to give less powers to supervisory authorities. This is not acceptable, especially given the possibly serious consequences of data processing by law-enforcement authorities and keeping in mind the numerous scandals regarding the infringements of data protection rules by law-enforcement agencies. Also, the harmonising effect of these provisions is missing.

A further difference is **Article 45(6)** of the proposed Directive, which allows supervisory authorities to charge fees for "vexatious" requests, as compared to "manifestly excessive" ones under the proposed Regulation (Article 52(6) there). Another difference is the publication of activity reports (**Article 47**): while under the Regulation, such reports will be public (Article 54 there), their counterparts under the Directive do not necessarily have to be published, only "be made available" to the Commission and the European Data Protection Board.

Article 48, dealing with mutual assistance of supervisory authorities is significantly shorter than the corresponding provision in the proposed Regulation (Article 55). Given that law-enforcement authorities often cooperate across borders, supervisory authorities should also have clear rules on mutual assistance.

(2) OUR RECOMMENDATIONS

- The most pressing changes need to be made to **Article 46**, which should be redrafted to include a list of powers that is aligned with the list of powers granted to supervisory authorities under the proposed Regulation (Article 53 there). If this is not possible, then at the very least the indicative list of powers ("such as") should be changed to a minimum list ("including").
- From the perspective of ensuring full political independence of supervisory authorities, it would be advisable to introduce an explicit clause in **Article 41** that would clarify that their

members should be appointed by the national parliaments. This can further help to remove supervisory authorities from political pressure (compared to the current wording, which also allows them to be appointed by the government). We have already suggested a similar change to the proposed Regulation.

- In **Article 45 (6)**, the word "vexatious" should be changed to "manifestly excessive", in line with the provisions in the proposed Regulation.
- **Article 47** should be amended to require publication of activity reports. This would increase transparency in an area where it is of paramount importance.
- **Article 48** should be brought in line with its counterpart in the General Data Protection Regulation, taking specificities of the law-enforcement sector into account where necessary.