1. Application of a directive

Rather than creating a single, comprehensive data protection regulation that sets the general rules for all personal data processing within the European Union, the Commission has opted to continue to distinguish between different categories of personal data processing: it has proposed to enact a regulation to replace the 1995 Data Protection Directive (the “Proposal Regulation”) and a directive to replace the 2008 Framework Decision (the “Proposal Directive”). The Proposal Regulation addresses data processing in the commercial sector and some parts of the public sector while the Proposal Directive addresses data processing in the law enforcement sector. The Faculty of Law has given its views on the Proposal Directive.1 Data processing in the context of national security has been excluded from the scope of both proposals.

The decision to attach different legal rules to different categories of personal data processing is controversial. This is because different categories of data often blur together which results in the legal rules being applied in artificial and arbitrary manner. For example, Passenger Name Record (PNR) data2 is first collected for commercial purposes and then used for law enforcement and

---

1 Remiss: Kommissionens förslag till dataskyddsdirektiv för de brottsbekämpande myndigheterna (KOM 2012 10 slutlig). Dnr SU 302-0688-12

2 A PNR is a file created by airline companies comprised of information on each passenger and his/her journey (e.g. name, billing information, address, meal preference etc.). Located in the airline’s reservation and departure control database, the PNR will allow the different agents within the air industry to recognize the passenger it is associated with, and the relevant information about his/her trip. For more, see, European
security purposes. The same is true for telecommunications data³. Yet, the European Court of Justice (ECJ) has distinguished PNR data from telecommunications data and found, in two widely criticized opinions, that PNR is not subject to the rules of the 1995 Data Protection Directive while telecommunications data is subject to the directive.⁴ And, even if one accepts that it is possible to distinguish between different categories of personal data, then ostensibly data collected in the context of law enforcement and security should be held to the highest levels of data protection standards. This is because in these contexts state actors are in a position to impose far greater liberty infringements than are possible by private actors in the commercial sector.

On the other hand, there exists some justification for creating specific rules for data processing in the context of law enforcement. That is, Member States require a certain flexibility to address the unique concerns that arise when processing personal data in this context. For example, law enforcement agencies may have a legitimate need to keep data for much longer periods (sometimes in perpetuity) than the commercial sector: this is because it is possible to link different pieces of data at different points in time in order to create evidence. Likewise, law enforcement agencies may also need to rely on data of a much lower quality ("hearsay") than the commercial sector in order to build evidence against suspects. The creation of specific rules, however, should not equate with a general lowering of data protection rights.

In either event, the use of a directive is certainly a step forward from the Framework Decision and will strengthen individual data protection rights for several reasons. First, unlike the Framework Decision, the Proposal Directive will not only be capable of having direct effect but it will also be subject to the general jurisdiction of the ECJ. Furthermore, enforcement proceedings may be taken by the Commission for any failure to transpose the Proposal Directive into domestic law.

The application of a directive is also beneficial to the extent it should encourage deeper cooperation and information sharing between the law enforcement authorities within the EU in accordance with the Stockholm Programme. This is because a directive will promote greater harmonization of the law by limiting the room that Member States have to manoeuvre when implementing its provisions. With a directive, a law enforcement agency in Member State A should not feel reluctant to share data with a law enforcement agency in Member State B because a directive will, at least ostensibly, guarantee that a relatively high level of data protection exists across all law enforcement bodies in the EU.

2. Scope of the proposal

2.1. Not limited to cross-border data processing

One of the biggest failures of the Framework Decision is that it is limited in scope insofar as the only transfers that fall within the ambit of its protection are those transfers of personal data that are exchanged between Member States. In other words, the processing of personal data that a Member State has gathered nationally is outside the ambit of the Framework Decision’s protection. This distinction does not exist in the relevant Council of Europe instruments such as:

---

³ Telecommunications data generally concerns personal data intercepted as a result of an individual’s use of the phone and internet.
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, its Additional Protocol regarding supervisory authorities and trans-border data flows and Recommendation No R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, adopted on 17 September 1987. The result of this limitation of scope has been to foster great complexity to data processing in this field.

Significantly, the Proposal Directive is not limited to cross-border data processing but applies to all processing activities carried out by competent authorities. In other words, the Proposal Directive will apply to both cross-border data processing and all data processing activities by the police and judiciary authorities at a purely national level. This can be seen as a major development to the extent that it will eliminate many difficulties for police and other competent authorities who have found it hard to distinguish between purely domestic and cross-border processing in practice and, as such, will ensure a more consistent application of the law throughout the EU.

### 2.2. Processing by Union institutions, bodies, offices and agencies

The Framework Decision excludes acts adopted on the basis of Title VI of the Treaty on European Union (TEU) that contain ad hoc data protection provisions. Likewise, the Proposal Directive does not apply to processing by Union institutions, bodies, offices and agencies which are permitted to create their own data protection rules (Article 2(b)). This means that information sharing laws pertaining to Europol, Eurojust, the Schengen Information System (SIS), the Customs Information System (CIS), as well as the Prum Decision all fall outside the scope of the Proposal Directive. This, of course, creates confusion in the field because it leaves open the question of which rules apply in certain real-world situations. In other words, it creates a fragmented and uncertain legal environment when it comes to the processing of certain data which may be subject to one or more of these different sets of data protection rules. The application of a regulation rather than a directive would not necessarily promote a more coherent legal framework because it might still be possible to exclude Union institutions if there exists good reason to do so.

### 3. Supervisory Authorities

The Framework Decision does not establish a supervisory body (mirroring, for example, the 1995 Directive's Article 29 Working Party). The Proposal Directive, does, however, establish supervisory authorities at Member State level and a European Data Protection Board (Chapter VI). There is concern, however, that these new data protection officials may subordinate legitimate law enforcement interests to privacy and data protection. It is therefore critical that these officials have knowledge in both law enforcement and data protection.

### 4. Distinguishing different categories of data and data subjects

Unlike the Framework Decision, the Proposal Directive requires that a distinction be made between data based on facts and data based on opinions or personal assessments. Furthermore, inspired by the Council of Europe's Recommendation No R (87), the Proposal Directive requires the distinction, as far as possible; between personal data of different categories of data subjects. This provision was not included in the Framework Decision.

These provisions recognize that different individuals and types of data may be entitled to various levels of data protection. Also, by categorizing data in this manner, it may be easier for law enforcement to abide by the purpose limitation principle when sharing the data with other agencies in the EU. Making all of these distinctions may, however, create added administration for the law enforcement authorities.
5. Profiling

The Framework Decision does not expressly refer to profiling; it only indirectly refers to it in Article 15 by way of discussing automated-decisions on individuals. The Proposal Directive, however, makes an explicit reference to profiling in Article 9 (Measures based on profiling and automated processing). It also attempts to define “profiling” at the outset of the proposal. This is a significant achievement because profiling operations in the law enforcement context are gaining importance and proper data protection regulation must keep pace.

6. Transparency

The Proposal Directive seeks to increase transparency by: first, requiring prior consultation with supervisory authorities; second, requiring data breach notifications and; third, introducing Data Protection Officers. Still, there is no requirement to notify individuals after the processing of their personal data is completed. Furthermore, Data Protection Impact Assessments have been taken out from the Proposal Directive, in comparison to its version leaked in November 2011. This is significant because PIAs have the potential to identify specific privacy risks and help government officials determine what, if any, controls are needed to mitigate those risks.

7. Transfers to third-countries

The Proposal Directive attempts to make the adequacy requirement more consistent and easy to apply. Because the Proposal Directive applies to both cross border and national processing of data, it would mean that the adequacy requirement is generally applicable throughout the EU (in this respect, the CoE Additional Protocol would seem to lose its meaning, at least for the EU Member States that have signed it). Furthermore, under the Proposal Directive, unlike in the Framework Decision, the Commission is permitted to make adequacy determinations. The effect of a Commission’s determination that a third country is “adequate” is that Member States will be able to send data there without any further safeguards being necessary.

Giving the Commission the authority to make adequacy determinations simplifies the adequacy procedure for Member States (who would only need to check whether the Commission has deemed a third country adequate rather than conducting its own assessment) and ensures a common approach to its implementation. That said, it seems to be somewhat of a political and bureaucratic fiction that some countries provide “adequate” data protection while others do not. To put it more bluntly: there is certainly a concern that the Commission will simply “rubber stamp” certain countries as “adequate” without genuinely assessing the third country’s data protection regime. It is also worth mentioning that allowing the Commission to make these adequacy determinations (along with checking the implementation and compliance with the Directive) makes the Commission the new “big player” in data protection. This raises the question: are Member States comfortable the Commission’s new role?

In the absence of a Commission determination that a third country is “adequate,” data transfers are authorized either where “appropriate safeguards with respect to the protection of personal data have been adduced in a legally binding instrument” or “the controller or processor has assessed all

---

5 Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows (November 8, 2001)(not fully ratified).
the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with respect to the protection of personal data.” With respect to the former, the Proposal Directive suggests in Article 36 that existing legal instruments in place between EU Member States and third countries must be renegotiated if they do not include “appropriate safeguards.” This interpretation seems particularly accurate in light of Article 60 which states that “international agreements concluded by Member States prior to the entry force of this Directive shall be amended, where necessary, within five years after the entry into force of this Directive.” Obviously, having to renegotiate bilateral agreements may be problematic for Member States (for example, both of the EU-US Mutual Legal Assistance Treaties contain clauses that explicitly restrict the EU from denying cooperation based on general data protection concerns).

Finally, the Proposal Directive states that a transfer may also take place if one of the derogations set forth in the Proposal Directive is applicable. For example, a derogation will apply if “the transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country.” Like the Framework Decision, these derogations are vaguely framed (e.g., what constitutes an “immediate and serious” threat?).

8. Liability and the right to compensation

Pursuant to Article 54, each Member State shall provide “that any person who has suffered damage as a result of an unlawful processing operation of an action incompatible with the provisions adopted pursuant to (the Proposal Directive) shall have the right to receive compensation from the controller or the processor for the damage suffered.” The Directive further provides for joint and several liability for all “controllers” or “processors” who violate the Directive and cause damage to data subjects (Article 54). Because “processors” includes any “natural or legal person” under Article 3(7) individual civil servants are subject to liability under the Directive. This may create a “chilling effect” on the willingness of law enforcement officials to collect information required for their investigations.

9. Conclusion

When viewed in comparison with the Framework Decision, the Proposal Directive can be seen to advance data protection rights. It includes all data processing activities carried out by national law enforcement authorities and not just transfers of personal data that are exchanged between Member States. This will not only create consistency in the real-world application of the law but will also ensure that the adequacy requirement is generally applicable to all third-country transfers. The Proposal Directive also establishes supervisory authorities, attempts to address the complicated issue of profiling and seeks to increase transparency in the field.

The Proposal Directive, however, could have gone much further towards strengthening individual data protection rights. By opting for a separate directive rather than a single regulation which encompasses general data protection rules for all personal data processing within the EU, the proposal adds additional complexity to the field that may undermine data protection objectives. Furthermore, the Proposal Directive fails to sufficiently clarify the procedure for sending data to third countries which is particularly disappointing in light of the increasingly global and networked environment. It also creates a lack of legal certainty to the extent that it does not apply to processing by Union institutions, bodies, offices and agencies.