



Opinion of the European Data Protection Supervisor

on the Proposal for a Directive of the European Parliament and of the Council amending Directives 89/666/EEC, 2005/56/EC and 2009/101/EC as regards the interconnection of central, commercial and companies registers

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular its Article 16,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data²,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 24 February 2011, the European Commission adopted a Proposal for a Directive of the European Parliament and of the Council amending Directives 89/666/EEC, 2005/56/EC and 2009/101/EC as regards the interconnection of central, commercial and companies registers³ ("Proposal") and subsequently consulted the EDPS.
2. The EDPS is pleased that he has been consulted as required by Article 28(2) of Regulation 45/2001 and that a reference to this Opinion is included in the preamble of the Proposal.

1.1 Objectives of the Proposal

¹ OJ 1995, L 281/31.

² OJ 2001, L 8/1.

³ For the sake of brevity, the "*central, commercial and companies registers*" will be referred to further in this Opinion as "*business registers*".

3. The aim of the Proposal is to facilitate and step up cross-border cooperation and information exchange among business registers in the European Economic Area and thereby increase transparency as well as the reliability of information available across borders. Efficient administrative cooperation procedures with regard to business registers is crucial in order to increase confidence in the European single market by ensuring a safer business environment for consumers, creditors and other business partners, reducing administrative burdens, and increasing legal certainty. Stepping up administrative cooperation procedures concerning business registers in Europe is particularly important in procedures for cross-border mergers, seat transfers and updating the registration of foreign branches where cooperation mechanisms are currently lacking or are limited.
4. To this end, the Proposal aims to amend three existing directives, as follows:
 - the amendments to Directive 2009/101/EC⁴ aim at facilitating cross-border access to official business information by (i) setting up an electronic network of business registers and (ii) determining a common minimum set of up-to-date information to be made available to third parties by electronic means via a common European multilingual platform/access point;
 - the amendments to Directive 89/666/EEC⁵ are intended to ensure that the business register of a company provides up-to-date information on the status of the company to the business register of foreign branches all across Europe; and finally,
 - the amendments to Directive 2005/56/EC⁶ aim to improve the administrative cooperation procedures related to between business registers in cross-border merger procedures.

1.2. Context of the Proposal

5. Business registers exist in every Member State; they are organised either at a national, regional or local level. In 1968 common rules were adopted to establish minimum standards for disclosure (registration and publication) of business information⁷. Since 1 January 2007, Member States also have to maintain electronic business registers⁸ and allow third parties to access the content of the register online.
6. Cooperation concerning business registers from different Member States is explicitly required by some European legal instruments in order to facilitate the cross-border

⁴ Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (OJ L 258, 1.10.2009, p. 11).

⁵ Eleventh Council Directive 89/666/EEC of 21 December 1989 concerning disclosure requirements in respect of branches opened in a Member State by certain types of company governed by the law of another State (OJ L 395, 30.12.1989, p. 36).

⁶ Directive 2005/56/EC of the European Parliament and of the Council of 26 October 2005 on cross-border mergers of limited liability companies (OJ L 310, 25.11.2005, p. 1).

⁷ Directive 2009/101/EC, cited above in full. Article 1 of the Directive limits the scope of the Directive's provisions to "companies incorporated with limited liability".

⁸ Directive 2003/58/EC of the European Parliament and of the Council of 15 July 2003 amending Council Directive 68/151/EEC, as regards disclosure requirements in respect of certain types of companies (OJ L 221, 4.9.2003, p. 13).

mergers of limited-liability companies⁹ and the cross-border seat transfer of the European Company (SE)¹⁰ and of the European Cooperative Society (SCE)¹¹.

7. In 1992 a voluntary cooperation mechanism was created with regard to business registers in Europe. By now the so-called European Business Register ("EBR")¹² combines official business registers from 19 Member States and six other European jurisdictions. Between 2006 and 2009, EBR took part in a research project called BRITE¹³ that had the objective of developing a technological platform for the interoperability of business registers throughout Europe. The Impact Assessment accompanying the Proposal, however, explains that EBR faces significant challenges as regards its expansion, financing and governance: according to the Impact Assessment, the current cooperation mechanism, in its present form, is not fully satisfactory for potential users.

1.3. Synergies with other initiatives

8. The Explanatory Memorandum accompanying the Proposal notes that the European e-Justice portal¹⁴ is to become the key point of access to legal information, legal and administrative institutions, registers, databases and other services in the EU. It further confirms that the Proposal is complementary to the e-Justice project and should contribute to easier access to business information to third parties through the portal.
9. According to the Impact Assessment, another relevant project with potential synergies is the Internal Market Information System (IMI).¹⁵ IMI is an electronic tool designed to support day-to-day administrative cooperation between public administrations in the context of the Services Directive (2006/123/EC) and the Professional Qualifications Directive (2005/36/EC). IMI is currently in the process of being expanded and could, according to the Impact Assessment, also support the enforcement of other directives including in the area of company law.

II. RELEVANT PROVISIONS OF THE PROPOSAL

10. Article 3 of the Proposal amends Directive 2009/101/EC in several respects. Of these, two amendments have significant relevance for data protection.

2.1. Publication of information via a common European electronic platform/access point

11. Article 2 of Directive 2009/101/EC as currently in force already requires that certain minimum information should be disclosed in a business register in each Member State so that third parties may be able to ascertain information concerning companies. As explained in Section 1.2 above, Member States also have to maintain electronic business registers and allow third parties to access the content of these registers online.

⁹ Directive 2005/56/EC, cited above in full.

¹⁰ Regulation (EC) No 2001/2157 of 8 October 2001 on the Statute for a European company (OJ L 294, 10.11.2001, p. 1).

¹¹ Regulation (EC) No 2003/1435 of 18 August 2003 on the Statute for a European Cooperative Society (OJ L 207, 18.08.2003, p. 1).

¹² <http://www.ebr.org/>.

¹³ <http://www.briteproject.eu>.

¹⁴ <https://e-justice.europa.eu/home.do>.

¹⁵ http://ec.europa.eu/internal_market/imi-net/index_en.html.

12. Article 2 lists eleven items of basic company information to be disclosed to the public, including the following:
- the instrument of constitution, statutes, and any amendments thereto,
 - capital subscribed,
 - accounting documents,
 - change in the registered office of the company,
 - winding up; declaration of nullity; appointment of liquidators; end of liquidation, striking off from register.
13. Importantly from the data protection point of view, Article 2 also requires disclosure of the "*appointment, termination of office and particulars*" (emphasis added) of the persons who are (i) authorised to represent the company and/or (ii) are otherwise involved in the company's "*administration, supervision or control*".
14. The list of items required to be disclosed under Article 2 has remained unchanged by the Proposal. Neither is it a new requirement that each Member State should make this information publicly available electronically. The novelty of the Proposal is that the information which has thus far been available in a fragmented manner, often only in local languages and via local websites, will now be easily accessible, via a common European platform/access point, in a multilingual environment.
15. To this effect, the Proposal would insert a new Article 3a into the Directive, to provide that "*Member States shall ensure that the documents and particulars referred to in Article 2 that have been filed with their register can be obtained, on application by any applicant, by electronic means through a single European electronic platform accessible from every Member State.*" The Proposal leaves all further details to delegated acts.

2.2. Inter-operability and inter-connection of business registers: establishment of an electronic network

16. The Proposal would also insert a new Article 4a into the same Directive 2009/101/EC, to provide that "*Member States shall take the necessary measures to ensure that the [business registers] are interoperable and form an electronic network*". The Proposal, again, leaves further details to delegated acts.

2.3. Provisions on data protection

17. To address data protection concerns, the Proposal would insert into the text of all three Directives to be amended a specific article on data protection requiring that "*[t]he processing of personal data carried out in the context of [the] Directive shall be subject to Directive 95/46/EC*".

III. EDPS COMMENTS AND RECOMMENDATIONS

3.1. Introduction: meeting the needs of both transparency and privacy

18. The EDPS shares the Commission's view that (i) the use of information and communication technologies may help increase efficiency of cooperation with regard to business registers and (ii) increasing accessibility of business register information may lead to increased transparency. Therefore, he supports the objectives of the Proposal. His comments are to be evaluated in light of this constructive approach.

19. At the same time, the EDPS also emphasizes that increased accessibility of personal data also leads to increased risks to personal data. For example, while correct identification of a company representative may be facilitated if his private address is disclosed, disclosure could also have a negative impact on this individual's right to the protection of personal data. This is especially so for personal data made widely available on the internet in digital form in multiple languages and via an easily accessible European platform/access point.
20. In the not so distant past, personal data from business registers (e.g. the name, address and specimen signature of a director) were disclosed to the public in a paper form and in a local language, following often only a personal visit of the applicant to a local registry office. It is important to recognize that this situation is qualitatively different from public disclosure of data in digital form via a nationwide electronic access point. Public disclosure of personal data via an easily accessible all-European platform/access points takes this one step even further, and further increases accessibility of information, as well as the risks to the protection of personal data of the individuals concerned.
21. Among the privacy risks present (due to easy availability of the data in digital form over a common electronic access point) are identity theft and other criminal activities, as well as the risk that the information disclosed may be unlawfully harvested and used by companies for commercial purposes that were not foreseen initially, after profiling the individuals concerned. Without adequate safeguards, the information may also be sold to others, or combined with other information and sold back to governments to be used for unrelated and undisclosed purposes (e.g. for tax law enforcement or other criminal or administrative investigations) without an adequate legal basis.¹⁶
22. For these reasons, it must be carefully assessed what personal information should be made available via the common European platform/access point, and what additional data protection safeguards - including technical measures to restrict search or download capabilities and data mining - should apply.

3.2 Essential data protection safeguards should be set forth in the Proposal itself and should not be left for delegated acts

23. As noted in Sections 2.1 and 2.2 above, the proposed Articles 3a and 4a of Directive 2009/101/EC are very general and leave many key issues to delegated acts.
24. Although the EDPS acknowledges the need for flexibility, and thus, also the need for delegated acts, he emphasises that the necessary data protection safeguards are essential elements which should be clearly and specifically provided for directly in the text of the proposed Directive itself. In this respect, they cannot be regarded as "non-essential elements" which may be included in subsequent delegated acts adopted under Article 290 of the Treaty on the Functioning of the European Union.
25. Therefore, the EDPS recommends that the data protection provisions of the Proposal should be more specific and go beyond simply referring to Directive 95/46 (see Sections 3.4 to 3.13). Additional provisions regarding the implementation of specific safeguards may then be included in delegated acts, on a basis of a consultation of the EDPS and,

¹⁶ Indeed, there is a developing market consisting of selling this kind of business information: service providers on this market score the trustworthiness of companies/individuals based on information collected from many places including business registers, court registers, insolvency registers, etc.

where appropriate, of national data protection authorities (see Sections 3.5, 3.6, 3.8, 3.9, 3.10, 3.12 and 3.13 below).

3.3. Other essential elements of the proposed measures should also be clarified in the Proposal itself

26. The Proposal is not only silent regarding key data protections safeguards; it is also very open-ended in other respects. In particular, it also leaves to delegated acts to determine essential elements of how it wishes to accomplish the proposed (i) interconnection of business registers and (ii) public disclosure of data.
27. Clarity on these other essential elements of the Proposal is a necessary precondition to the adoption of adequate data protections safeguards. Therefore, the EDPS recommends that these essential elements should be set forth in the proposed Directive itself (see Sections 3.4 and 3.5 below).

3.4 Governance: roles, competences and responsibilities should be clarified in the proposed Directive

28. For the moment, the Proposal leaves to delegated acts to determine the rules concerning the governance, management, operation and representation of the electronic network.¹⁷
29. While the Impact Assessment and the Explanatory Memorandum identify some synergies with IMI and the E-Justice portal, the text of the proposed Directive leaves open the door for various options to allow any or all of these synergies to materialize, including a re-design of the EBR, the use of IMI for certain data exchanges, and/or the use of the e-Justice portal as the platform/access point for providing information from the business registers to the public.
30. Other options are also not excluded, such as issuing a tender to award the right to design and operate the electronic network, or the Commission taking a direct role in designing and operating the system. Member State representatives may also be involved in the governing structure of the electronic network.
31. In addition, although the Proposal, in its current form, foresees a "*single European electronic platform*" (emphasis added), it is not excluded that the text may be modified further in the legislative procedure to provide for a more decentralized structure.
32. The EDPS also notes that although the current Proposal does not specifically address the issue of interconnecting business registers with other databases (such as, for example, with land registers or civil registers), this is certainly a technical possibility, and something that is already happening in some Member States.¹⁸
33. The choice for one or another of these options may lead to a completely different structure of governance of the electronic network and of the electronic tool to be used for public disclosure. This, in turn, leads to different roles and responsibilities of the parties

¹⁷ See the proposed text for Article 4(a)(3)(a) of Directive 2009/101/EC.

¹⁸ Considering that interconnection is not currently foreseen in the Proposal, the EDPS will not discuss this issue further in his Opinion at this stage. Nevertheless, he calls attention to the fact that should inter-connection be contemplated, this may require a separate proportionality analysis, and the adoption of additional adequate data protection safeguards.

involved, resulting also in different roles and responsibilities from the data protection point of view.

34. In this respect, the EDPS emphasises that in any situation where personal data are processed, it is crucial to correctly identify who the "controller" is. This was also emphasized by the Article 29 Data Protection Working Party in its Opinion 1/2010 on the concepts of "controller" and "processor"¹⁹. The primary reason why the clear and unambiguous identification of the controller is so crucial is that it determines who shall be responsible for compliance with data protection rules and is also relevant to identify which law is applicable.²⁰
35. As noted in the Article 29 Working Party Opinion, "*[i]f it is not sufficiently clear what is required from whom - e.g. no one is responsible or a multitude of possible controllers - there is an obvious risk that too little, if anything, will happen and that the legal provisions will remain ineffective*".
36. The EDPS emphasizes that clarity is especially needed in situations where multiple actors are involved in a cooperative relationship. This is often the case with EU information systems used for public purposes where the purpose of processing is defined in EU law.
37. For these reasons, the EDPS recommends to establish, in the text of the proposed Directive itself, and in a specific, clear and unambiguous manner:
- whether the electronic network will be operated by the Commission or by a third party and whether it will have a centralized or decentralized structure;
 - the tasks and responsibilities of each party involved in the data processing and the governance of the electronic network, including the Commission, Member State representatives, holders of business registers in Member States and any third parties; and
 - the relationship between the electronic system foreseen in the Proposal and other initiatives such as IMI, the e-Justice portal and the EBR.
38. From the data protection perspective, these clarifications should also be specific and unambiguous with a view to establish, on a basis of the proposed Directive itself, whether a particular actor should be regarded as a "controller" or as a "processor".
39. In principle, the Proposal should explicitly contribute to establish, as it seems from the current draft as a whole, that the holders of the business registers as well as the operator/s of the system should each be regarded as a data controller with respect to their own activities. That being said, considering that presently the Proposal does not describe the governance structure and does not define who will be the operator/s of the electronic system, it cannot be excluded that some of the entity or entities that will ultimately operate the system at the practical level, will act as a processor rather than as a controller. This may be the case, especially, if this activity is outsourced to a third party who will act strictly upon instructions. In any case, it appears that there remain multiple data

¹⁹ See Article 2(d) and (e) of both Directive 95/46 and of Regulation 45/2001; as well as Opinion 1/2010 of 16 February 2010 of the Article 29 Data Protection Working Party on the concepts of "controller" and "processor" (WP169).

²⁰ Considering that data protection laws are not fully harmonized across Europe, the identity of the controller is relevant to determine which national legislation is applicable. In addition, it is also relevant to determine whether Directive 95/46 or Regulation 45/2001 applies: if the Commission is (also) a controller, then Regulation 45/2001 will (also) be applicable, as explained in Section 3.11 below.

controllers, at least one in each Member State: the entities who maintain the business registers. The fact that there may be other (private) entities involved as operators, "distributors", or otherwise, does not change this aspect. In any event, this should be specified in the proposed Directive, to ensure clarity and legal certainty.

40. Last but not least, the Proposal should also describe more specifically and more comprehensively the responsibilities that derive from these roles. For example, the operator/s' role in ensuring that the system is designed in a privacy-friendly way as well as its coordinating role with respect to data protection issues should be included in the Proposal.
41. The EDPS notes that all these clarifications will be also relevant to establish which data protection supervisory authorities are competent and for which processing of personal data.

3.5 Framework and legal basis for data-flows/administrative cooperation procedures should be defined in the proposed Directive

42. It appears that in its present form, the electronic network is not foreseen to make all information held in each business register to be automatically available to all other business registers in all other Member States: the Proposal merely requires the interconnection and interoperability of business registers, and thus, provides for the conditions to allow information exchanges and access in the future. To ensure legal certainty, the Proposal should clarify whether this understanding is correct.
43. In addition, the Proposal also does not specify what data flows/administration cooperation procedures may take place via the interconnected business registers.²¹ The EDPS understands that some flexibility may be needed to ensure that needs that may arise in the future can be accommodated. With that said, the EDPS considers it essential that the Proposal specifies the framework for data-flows and administrative cooperation procedures that may take place in the future using the electronic network. This is particularly important in order to ensure that (i) any data exchange will be made on a solid legal basis, and that (ii) adequate data protection safeguards are provided for.
44. According to the EDPS, any data exchange or other data processing activity using the electronic network (e.g. public disclosure of personal data via the common platform/access point) should be based on a binding EU act adopted on a solid legal basis. This should be clearly laid down in the proposed Directive.²²

3.6 Other key issues left to delegated acts should also be discussed in the proposed Directive

45. In addition, the Proposal provides that delegated acts determine the following issues²³:

²¹ This is with the exception, to some extent, of data exchanges in case of cross-border mergers, seat transfers and updates of branch information, which are specifically discussed in the Proposal.

²² In this respect, if there is a potential need for data processing in an Internal Market area not covered by a specific Union act, the EDPS calls for further reflection on the modalities of a legal framework which would allow, perhaps in combination with general Treaty provisions, specific provisions in the proposed Directive, and further delegated acts, to provide an adequate legal basis from the data protection perspective. It should also be specified in the proposed Directive whether the business registers may use the electronic network and the common access point to exchange or publicly disclose personal data not foreseen in a Union act but permitted or required under national law.

²³ See the proposed text for Article 4(a)(3) of Directive 2009/101/EC.

- the conditions for countries outside the European Economic Area to participate in the electronic network;
 - the minimum security standards for the electronic network; and
 - the definition of standards on format, substance and limits for storing and retrieving the documents and particulars that enables automated data exchange.
46. With regard to the first and the second indent, the EDPS considers that certain essential safeguards should be provided for in the proposed Directive itself (see Sections 3.12 and 3.13 below). Further details then can be set forth in delegated acts.
47. With regard to automated data exchanges, the EDPS is pleased that the Proposal requires delegated acts to provide for "*definition of standards on format, substance and limits for storing and retrieving the documents and particulars that enables automated data exchange*".
48. To provide for more clarity in this regard, the EDPS recommends that the proposed Directive itself clearly specifies that the electronic network enables (i) specific manual case-by-case data exchanges between business registers (as provided in an EU act such as in case of a merger or a seat transfer); and (ii) automated data transfers (as provided in an EU act such as in case of updating information in the register of foreign branches).
49. To further enhance clarity, the EDPS also recommends that the proposed text for the relevant Article 4(a)(3)(i) of Directive 2009/101/EC is modified to ensure that (i) delegated acts will comprehensively cover both manual and automated data exchanges and (ii) all processing operations that may involve personal data (not only storage and retrieval) are covered; and that (iii) specific data protection provisions in delegated acts will also ensure the practical application of relevant data protection safeguards.
50. To illustrate, Article 4(a)(3)(i) may, for example, be modified to read as follows:
- "(i) format, substance and limits for any manual or automated data processing operations taking place using the network, including transferring, storing and retrieving information; as well as specific measures that may be necessary to ensure the practical application of relevant data protection safeguards"*.

3.7. The categories of personal data processed should be clarified further in the proposed Directive

51. As a preliminary remark, the EDPS emphasises that while the names (and possibly, other details, such as private addresses) of the representatives of the companies (and other individuals involved in the companies' governance) undoubtedly constitute the most obvious personal data that may be processed by the electronic network and/or disclosed publicly via the common electronic platform/access point, these are by no means the only personal information held in business registers.
52. First of all, some of the documents listed in Article 2 of Directive 2009/101/EC (e.g. the instrument of constitution, statutes and accounting documents) may also contain personal data of other individuals. These data may include, among others, names, addresses, possibly identification numbers and dates of birth, and even scans of handwritten signatures, of a variety of individuals, including the individuals who founded the

company, the companies' shareholders, lawyers, accountants, employees or notaries public.

53. Second, company data, when linked to the name of an individual (such as a director), could also be considered as personal data relating to this individual. For example, if the data from the business register show that a particular individual is on the board of directors of a company that is undergoing liquidation, this information is also relevant for that individual.
54. To ensure clarity as to what personal data are processed, and to ensure that the range of the data processed are proportionate to the objectives of the Proposal, the EDPS recommends the clarifications set forth further in this Section 3.7.

The phrase "particulars of persons" should be clarified in the proposed Directive

55. Article 2 of Directive 2009/101/EC does not define what "*particulars*" of the individuals concerned (company representatives and others involved in corporate governance) are required to be disclosed.
56. Indeed, the different language versions of the Proposal show significant differences even with respect to the translation of the phrase "*particulars of persons*". For example, the phrase reads as "*l'identité des personnes*" (i.e. identity of the persons) in French, "*le generalità delle persone*" (i.e. personal details such as name and surname) in Italian, "*személyek adatai*" (i.e. data of the individuals) in Hungarian, "*de identiteit van de personen*" (i.e. identity of the persons") in Dutch and "*identitatea persoanelor*" (i.e. identity of the persons) in Romanian.
57. Moreover, in some Member States the private addresses of company directors and/or other individuals such as some shareholders are routinely made publicly available on the internet. In some other Member States this information is kept confidential by the business register to which the information is submitted, for confidentiality concerns, including for fear of identity theft.
58. The EDPS recommends modifying Article 2 of Directive 2009/101/EC in order to clarify what, if any, personal data, in addition to the names of the individuals concerned (company representatives and others involved in corporate governance) are required to be disclosed. In doing so, the need for transparency and accurate identification of these individuals should be carefully considered but must also be balanced against other competing concerns such as the need to protect the privacy of the individuals concerned.²⁴
59. Should no agreement be reached due to the variations in national practices, Article 2 should at least be modified to require that "*the full name of the individuals concerned, and - if specifically required by national law - further data necessary for their identification*" should be disclosed. It will then be clear that it is left to each Member State to decide, in national legislation, what, if any, "*particulars*" in addition to the names are to be

²⁴ The proportionality assessment should be carried out, in particular, taking into account the criteria established by the European Court of Justice in *Schecke and Eifert* (ECJ 9 November 2010, joined Cases C-92/09 and C-93/09; see, in particular, paragraphs 81, 65 and 86). In *Schecke*, the ECJ underlined that derogations and limitations in relation to the protection of personal data must apply only in so far as it is strictly necessary. The ECJ further considered that the institutions should explore different methods of publication in order to find the one which would be consistent with the purpose of the publication while causing the least interference with the data subjects' right to private life in general and to protection of personal data in particular.

disclosed, and that additional personal data will only be required to be disclosed if this is necessary for identification of the individuals concerned.

60. Alternatively, and considering that Article 2 lists "*minimum information*" rather than fully harmonizing the contents of business registers across Europe, the phrase "*particulars of persons*" could simply be replaced with the phrase "*full names of persons*". It would be then also up to each Member State to decide, what, if any, additional information they wish to disclose.

The phrase "administration, supervision or control" should be clarified

61. Article 2 of Directive 2009/101/EC also requires information disclosure about persons involved in the company's "*administration, supervision or control*". Based on this broad formulation, it is not entirely clear whether information regarding shareholders is required to be disclosed: in particular, information about shareholders who have (i) a significant, influencing, or controlling share beyond a certain threshold or (ii) by virtue of golden shares, specific contractual arrangements or otherwise have an effective control/influence over the company.
62. The EDPS understands that a broad formulation is required to cover the wide variety of corporate governance structures that currently exist for companies with limited liability in the different Member States. With that said, legal certainty about the categories of individuals whose data that may be disclosed is essential from the data protection point of view. Therefore, the EDPS recommends modifying Article 2 of Directive 2009/101/EC in order to clarify what, if any, personal data regarding shareholders are required to be disclosed. In doing so, a proportionality analysis under *Schecke* (as noted above) must also be carried out.

Information disclosure beyond the minimum required; blacklists

63. Although the Proposal does not require exchange or public disclosure of personal data beyond the minimum requirements set forth in Article 2 of Directive 2009/101/EC, it does not exclude either that Member States, if they choose to, can require that their business registers process or disclose further personal data and make such data available also via the common European platform/access point and/or exchange such data with business registers in other Member States.
64. This is a particularly sensitive issue with respect to "blacklists". In some countries, the electronic register also functions, *de facto*, as a sort of "black-list" and can be searched by any third party via an electronic portal for information on company representatives who have been banned from their activities.
65. To address this issue, the EDPS recommends clarifying in the Proposal whether and to what extent Member States may eventually publicly disclose more information via the common portal and/or may eventually exchange more information with each other, based on their own national laws, if they choose to. In this case, a strict proportionality assessment (see *Schecke*, cited above) should be based on national law, and also take into account, as a consideration, the objectives of the internal market.
66. In addition, the EDPS suggests binding the use of these powers to a role to be played by national data protection authorities, for instance, by consultation.

67. Finally, the EDPS emphasises that if a European scheme were to be foreseen to specifically require such "black-lists", this should be specifically set forth in the proposed Directive.²⁵

3.8. Guarantees to ensure purpose limitation; safeguards against harvesting data, data mining, data combination, and overboard searches

68. The EDPS recommends that the proposed Directive should specifically provide that in all cases where personal data are publicly disclosed or otherwise shared among business registers, adequate safeguards should be provided, in particular, against harvesting data, data mining, data combination, and overboard searches, to ensure that personal data that have been made available for purposes of transparency will not be misused for additional, unrelated purposes.²⁶

69. The EDPS particularly emphasizes the need to consider technological and organizational measures following the principle of privacy by design (see Section 3.14 below). The practical implementation of these safeguards may be left to delegated acts. However, the principles should be set forth in the proposed Directive itself.

3.9 Information to data subjects and transparency

70. The EDPS recommends that the proposed Directive contain a specific provision requiring that information under Articles 10 and 11 of Directive 95/46 (and corresponding provisions of Regulation 45/2001, if relevant) should be provided to data subjects in an effective and comprehensive manner. In addition, and depending on the governance structure to be agreed upon and the roles and responsibilities of the different parties involved, the proposed Directive may specifically require that the operator of the system should take a proactive role in providing notice and other information to data subjects on its website, also "on behalf of" business registers. Further details may be included in delegated acts, if necessary, or left to be established in a data protection policy.

3.10 Rights of access, rectification and erasure

71. The Proposal should at least include a reference to the requirement of developing the modalities of an arrangement (in delegated acts) to enable data subjects for making use of their rights. Reference should also be made to the possibility for building a data protection module and the possibility of privacy by design solutions for cooperation among authorities regarding access rights, as well as "empowerment of data subjects" where relevant.

3.11 Applicable law

72. Considering that it is possible that the Commission or another EU institution/body may also process personal data in the electronic network (e.g. by acting as an operator of the network, or by retrieving personal data from it), a reference should also be made to Regulation 45/2001.

²⁵ Considering that this is not currently foreseen in the Proposal, the EDPS will not discuss this issue further in his Opinion at this stage. Nevertheless, he calls attention to the fact that should this be contemplated, this may require a separate proportionality analysis, and the adoption of additional adequate data protection safeguards.

²⁶ See Article 6(b) of Directive 95/46 and Regulation 45/2001.

73. It should also be clarified that Directive 95/46 applies to the business registers as well as other parties acting under their national laws in Member States, whereas Regulation 45/2001 applies to the Commission and other EU institutions and bodies.

3.12. Transfers of personal data to third countries

74. With respect to transfers of personal data by the holder of a business register in the EU to the holder of a business register in a third country that does not provide an adequate level of protection for personal data, the EDPS, first of all, emphasises that it is important to distinguish between two situations:

- cases where the personal data are already available in a public register (such as via the common European platform/access point), and
- cases where the personal data are not publicly available.

75. For the first case, Article 26(1)(f) of Directive 95/46 allows an exception when "*transfer is made from a [public] register*", subject to respect for certain conditions. For example, if the holder of a business register in a European country wishes to transfer a particular set of personal data (e.g. in connection with registration of foreign branches) to the holder of a business register in a third country, and the same data would already be publicly available, in any event, the transfer should be possible even if the third country in question does not provide an adequate level of protection.

76. For the second case, the EDPS recommends that the Proposal clarifies that transfers of data that are not publicly available can only be made to entities or individuals in a third country that does not afford adequate protection if the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regard the exercise of the corresponding rights. Such safeguards may in particular result from appropriate contractual clauses in place under Article 26(2) of Directive 95/46.²⁷ In cases where such data transfers to third countries systematically involve data shared between business registers in two or more EU countries, or where an action at EU level is otherwise desirable, a negotiation of contractual clauses could also take place at the EU level (Article 26(4)).

77. The EDPS emphasises that other derogations such as the one where (Article 26(d)) "*transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims*", should not be used to justify systematic data transfers using the electronic network to third countries.

3.13. Accountability and privacy by design

78. The EDPS recommends that the Proposal specifically refers to and strives to implement the principle of accountability²⁸ and establishes a clear framework for adequate internal mechanisms and control systems to ensure data protection compliance and provide evidence thereof, such as:

²⁷ If it is possible that in some cases the Commission may be among the actors which can transfer the data to third countries, a reference should also be made to Article 9(1) and 9(7) of Regulation 45/2001.

²⁸ See Section 7 of the EDPS Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions-"A comprehensive approach on personal data protection in the European Union", issued on 14 January 2011, in http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf.

- carrying out a privacy impact assessment (also including a security risk analysis) before designing the system;
- adopting and updating, as necessary, a formal data protection policy (implementing rules) , also with regard to a security plan;
- carrying out periodic audits to assess continued adequacy of and compliance with the data protection and security policy;
- making public (at least partially) the results of these audits to reassure stakeholders with respect to data protection compliance; and
- notifying data breaches and other security incidents.

79. As to privacy by design²⁹, the Proposal should specifically refer to this principle, and it should also materialise this commitment into concrete actions. In particular, the Proposal should provide that the electronic network must be safely and soundly built so it has embedded by default a wide range of privacy safeguards. A few possible examples of privacy by design safeguards include the following:

- a decentralized approach whereby data are only stored in a "master" source and each "distributor" only retrieves data from this "master" source (to ensure that the data are up-to-date);
- automatic processes that search for inconsistencies and inaccuracies of information;
- limited search capabilities to index only data that are proportional and adequate to the purpose;
- other safeguards to prevent/restrict bulk downloading, data mining, overboard searches, and ensure adequate purpose limitation; safeguards to prevent or restrict the possibilities of third parties to use the search interface to harvest data and profile individuals (e.g. "captcha"³⁰ or a registration requirement for payment);
- embedded system functionality to make it easier for data subjects to exercise their rights effectively; embedded functionalities for the business registers to coordinate amongst themselves with respect to data subject access requests;
- procedures to handle information about applicants who downloaded information from the public register in a secure and privacy-friendly way; and
- audit/trail mechanisms.

IV. CONCLUSIONS

80. The EDPS supports the objectives of the Proposal. His comments are to be evaluated in light of this constructive approach.

81. The EDPS emphasises that the necessary data protection safeguards should be clearly and specifically provided for directly in the text of the Directive itself, since he considers them essential elements. Additional provisions regarding the implementation of specific safeguards then can be set forth in delegated acts.

82. The issues of governance, roles, competences, and responsibilities need to be addressed in the proposed Directive. To this end, the proposed Directive should establish:

²⁹*Idem.*

³⁰ A "captcha" is a type of challenge-response test used in computing as an attempt to ensure that the response is not generated by a computer.

- whether the electronic network will be operated by the Commission or by a third party and whether it will have a centralized or decentralized structure;
- the tasks and responsibilities of each party involved in the data processing and the governance of the electronic network, including the Commission, Member State representatives, the holders of business registers in Member States and any third parties;
- the relationship between the electronic system foreseen in the Proposal and other initiatives such as IMI, the e-Justice portal and the EBR; and
- specific and unambiguous elements to determine whether a particular actor should be regarded as a "controller" or as a "processor".

83. Any data processing activity using the electronic network should be based on a binding legal instrument such as a specific Union act adopted on a solid legal basis. This should be clearly set forth in the proposed Directive.

84. Provisions on applicable law should be clarified and include reference to Regulation 45/2001.

85. With regard to transfers of personal data to third countries, the Proposal should clarify that in principle, and with the exception of cases falling under Article 26(1)(f) of Directive 95/46, transfers can only be made to entities or individuals in a third country that does not afford adequate protection if the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regard the exercise of the corresponding rights. Such safeguards may in particular result from appropriate contractual clauses in place under Article 26 of Directive 95/46.

86. Further, the Commission should carefully assess what technical and organizational measures to take to ensure that privacy and data protection are "designed" into the architecture of the electronic network ("privacy by design") and that adequate controls are in place to ensure data protection compliance and provide evidence thereof ("accountability").

87. Other recommendations of the EDPS include:

- the proposed Directive should clearly specify that the electronic network should enable (i) on one hand, specific manual data exchanges between business registers; and, (ii) on the other hand, automated data transfers. The Proposal should also be modified to ensure that (i) delegated acts will comprehensively cover both manual and automated data exchanges and (ii) all processing operations that may involve personal data (not only storage and retrieval); and that (iii) specific data protection provisions in delegated acts will ensure the practical application of relevant data protection safeguards;
- the Proposal should modify Article 2 of Directive 2009/101/EC to clarify what, if any, personal data, in addition to the names of the individuals concerned are required to be disclosed. It should be also clarified whether data regarding shareholders are required to be disclosed. In doing so, the need for transparency and accurate identification of these individuals should be carefully considered but must also be balanced against other competing concerns such as the need to protect the right to the protection of personal data of the individuals concerned;

- it should be clarified in the Proposal whether Member States may eventually publicly disclose more information via the common portal (and/or exchange more information with each other) based on their own national laws, subject to additional data protection safeguards;
- the proposed Directive should specifically provide that personal data that have been made available for purposes of transparency will not be misused for additional, unrelated purposes and that to this effect, technological and organizational measures should be implemented, following the principle of privacy by design;
- the Proposal should also include specific safeguards with respect to notice provision to data subjects as well as a requirement to develop the modalities of an arrangement to enable data subjects to make use of their rights in delegated acts.

Done in Brussels, on 6 May 2011.

(signed)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor