Annex

Comments on "Protection of personal data within the financial services providers" (page 43 et seq. of the Draft EA)

1) The Working Party welcomes the emphasis put by the Draft EA on basic data protection principles in particular in paragraph 251. The WP29 wishes to add that a relevant role is also played by the principle of purpose limitation according to which personal data are to be collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes, as broadly described in its Opinion 03/2013 (WP203). The WP29 also stresses the importance of the principle of proportionality which requires that the processing should not exceed the limits of what is appropriate and necessary in order to achieve the intended legitimate purposes. Proportionality should also be considered in respect of data retention. Appropriate policies should ensure that data retention is "proportionate" to the legitimate aim pursued and that data are kept for no longer than is necessary for such purpose. This fundamental principle should be valid in both the general principles on the protection of personal data within the financial service providers (page 43 of the Draft EA) and in the principles on Credit reporting systems' data sharing (page 45 et seq.).

2) Regarding the role of supervisory authorities (paragraph 252), the WP29 supports the fact that supervisory authorities should perform their duties in full independence and with adequate resources and powers. Such elements are indeed essential to ensure effective data protection compliance. It emphasises that together with their inspections powers, appropriate sanction powers are also an important component to ensure compliance.

3) With regard to paragraph 256 and 269, the WP29 would like to provide clarification regarding consent and, more generally, the legal basis for making data processing legitimate, as foreseen by the EU data protection framework, in particular Directive 95/46.
More than a "right" as stated in the document, consent is one of the prerequisites for data processing to be legitimate. In order to be valid, consent to the processing of personal data should not only be informed but also specific and freely given. The data subject's consent for the processing of personal data related to him/her should be separate from other terms and conditions and founded on adequate information.
Consent is not the only legal basis for processing personal data foreseen by the EU framework. The performance of a contract to which the data subject is party or the legitimate interest pursued by data controller or by the third party to whom the data are disclosed could be an appropriate legal basis alternative to consent (see e.g. Article 7 of Directive 95/46). For example, the processing carried out by credit reporting systems could be based on the data controller's legitimate interest in knowing whether anyone applying to it for credit has a record of failing to repay a loan, provided that such interest is not overridden by the data subject's fundamental rights and specific safeguards are in place to uphold those rights. As highlighted in its Opinion 6/2014 on the legitimate interest (WP217) and Opinion 15/2011 on the notion of consent (WP187), the Working Party highlights that having an appropriate legal ground does not relieve the data controller of its obligations with regard to fairness, lawfulness, necessity and proportionality, or ensuring data quality.

The Working Party also recalls that the duty to inform data subjects on the processing of data related to them – which should at least concern the identity and usual residence of the data controller, the main purposes of the processing, the existence of data subjects' rights and the recipients to whom the data may be communicated- is a general one, and should be respected regardless the legal basis (consent or others) of the processing.

4) A "Privacy Impact Assessment" (paragraph 257), should be carried out by authorities when developing legislation to assess the implications of new legislation on data subjects and identify any data protection problems. The Working Party seizes the opportunity to emphasise that an important step of the evaluation of the impact of new legislation on data subjects is the attribution to the competent supervisory authorities of the power to give opinion on proposals for administrative and legislative measures involving the processing of personal data in order to ensure the compliance of the intended processing with data protection framework and mitigate the risks for the data subjects.
It also underlines that, beyond the process of developing legislation, a "Privacy Impact Assessment" should be carried out by controllers – either public or private - before engaging in data processing. Such assessment would consist of a risk analysis of the potential impact of the intended processing operations on the data subject's rights, in order to prevent or minimize the risk of interference with those rights.

5) In respect of paragraph 261, regarding the roles of controllers and processors also in view of the allocation of respective responsibilities, it is important to emphasise that the chosen processor should provide for "appropriate" safeguards (rather than "sufficient") to meet the requirements of data protection relevant laws and that it processes the data only under the instructions of the financial services. The Working Party recalls its Opinion 1/2010 (WP169) on the concepts of "controller" and "processor" where these two notions are examined and which highlights the need to allocate responsibility in such a way that compliance with data protection rules is sufficiently ensured in practice.

Comments on Credit Reporting Systems data sharing (page 45 et seq. of EA).

6) With regard to the specific measures that credit reporting systems (CRSs) should adopt to ensure an adequate level of data quality – in terms of accuracy, completeness and updates (paragraph 268), it should be noted that data quality also requires that only relevant and not excessive personal data should be processed in accordance with the legitimate purpose of the processing. Moreover, proportionality is particularly important when it comes to registration and processing of personal data about someone's debts and credit rating, since such operations can lead to exclusion of consumers.

7) The document considers data dispute resolution mechanisms (both judicial and extrajudicial) (paragraph 270). In such context it is important to underline the role of supervisory authorities which, in the light of their competence and technical skills, may hear claims lodged by data subjects concerning the protection of their data protection rights.

8) The document states that the data usage for marketing purposes is allowed only if it is permitted by the law/regulations (paragraph 272). The Working Party wishes to recall the importance of ensuring that data subjects are able to exercise their right to opt-out with regard to the processing of their personal data for marketing purposes. The data subject should be adequately informed on the existence of such right.

9) Regarding the retention of data by CRSs, which is referred to in paragraph 274, it is particularly important to signal that appropriate policies should be in place to ensure that such retention is "proportionate" to the legitimate aim pursued and that data are kept for no longer than is necessary for such purpose.

10) The WP29 wishes to underline that in the realm of data subject's right to access to his/her personal data, it should be also provided that the data subject has the right to obtain knowledge of the logic involved in any automatic processing of her/his personal data when automated decisions are taken concerning her/him. Such a right is particularly important in respect of those operations contributing to the attribution of credit scores or statistical credit risk models based on automated techniques and other systems which may lead to the denial of credit.