3 Quality and integrity

Each Party shall take reasonable steps to ensure that personal data are maintained with such accuracy and completeness and are as up to date as is necessary and appropriate for the lawful processing of the personal data, having regard to the purposes for which they are processed.

4 Sensitive data

Processing by a Party of personal data revealing racial or ethnic origin, political opinions or religious or other beliefs, or trade union membership; genetic data; biometric data considered sensitive in view of the risks involved; or personal data concerning health or sexual life; shall only take place under appropriate safeguards to guard against the risk of unwarranted prejudicial impact from the use of such data, in particular against unlawful discrimination.

5 Retention periods

Each Party shall retain the personal data only for as long as necessary and appropriate in view of the purposes of processing the data pursuant to paragraph 2. In order to meet this obligation, it shall provide in its domestic legal framework for specific retention periods or periodic review of the need for further retention of the data.

6 Automated decisions

Decisions producing a significant adverse effect concerning the relevant interests of the individual to whom the personal data relate may not be based solely on automated processing of personal data, unless authorised under domestic law and with appropriate safeguards that include the possibility to obtain human intervention.

7 Data security and security incidents

a Each Party shall ensure that it has in place appropriate technological, physical and organisational measures for the protection of personal data, in particular against loss or accidental or unauthorised access, disclosure, alteration or destruction ("security incident").

b Upon discovery of a security incident in which there is a significant risk of physical or non-physical harm to individuals or to the other Party, the receiving Party shall promptly assess the likelihood and scale thereof and shall promptly take appropriate action to mitigate such harm. Such action shall include notification to the transferring authority or, for purposes of Chapter II, section 2, the authority or authorities designated pursuant to paragraph 7.c. However, notification may include appropriate restrictions as to the further transmission of the notification; it may be delayed or omitted when such notification may endanger national security, or delayed when such notification may endanger measures to protect public safety. Such action shall also include notification to the individual concerned, unless the Party has taken appropriate measures so that there is no longer a significant risk. Notification to the individual may be delayed or omitted under the conditions set out in paragraph 12.a.i. The notified Party may request consultation and additional information concerning the incident and the response thereto.

c Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe the authority or authorities to be notified under paragraph 7.b for the purposes of Chapter II, section 2; the information provided may subsequently be modified.

8 Maintaining records

Each Party shall maintain records or have other appropriate means to demonstrate how an individual's personal data are accessed, used and disclosed in a specific case.

9 Onward sharing within a Party

a When an authority of a Party provides personal data received initially under this Protocol to another authority of that Party, that other authority shall process it in accordance with this article, subject to paragraph 9.b.

b Notwithstanding paragraph 9.a, a Party that has made a reservation under Article 17 may provide personal data it has received to its constituent States or similar territorial entities provided the Party has in place measures in order that the receiving authorities continue to effectively protect the data by providing for a level of protection of the data comparable to that afforded by this article.

c In case of indications of improper implementation of this paragraph, the transferring Party may request consultation and relevant information about those indications.

10 Onward transfer to another State or international organisation

a The receiving Party may transfer the personal data to another State or international organisation only with the prior authorisation of the transferring authority or, for purposes of Chapter II, section 2, the authority or authorities designated pursuant to paragraph 10.b.

b Each Party shall, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, communicate to the Secretary General of the Council of Europe the authority or authorities to provide authorisation for purposes of Chapter II, section 2; the information provided may subsequently be modified.

11 Transparency and notice

a Each Party shall provide notice through the publication of general notices, or through personal notice to the individual whose personal data have been collected, with regard to:

i the legal basis for and the purpose(s) of processing;

ii any retention or review periods pursuant to paragraph 5, as applicable;

iii recipients or categories of recipients to whom such data are disclosed; and