

**COMP Article 32a (-33, first Article of Section 3 of Chapter IV)
17.10.2013**

**Article 32a
Respect to Risk**

1. The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks.

2. The following processing operations are likely to present specific risks:

(a) processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;

(b) processing of special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large scale filing systems;

(c) profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;

(d) processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

(e) automated monitoring of publicly accessible areas on a large scale;

(f) other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2);

(g) where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject;

(h) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects;

(i) where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.

3. According to the result of the risk analysis:

(a) where any of the processing operations referred to in paragraph 2 (a) or (b) exist, controllers not established in the Union shall designate a representative in the Union in line with the requirements and exemptions laid down in Article 25;

(b) where any of the processing operations referred to in paragraph 2 (a), (b) or (h) exist, the controller shall designate a data protection officer in line with the requirements and exemptions laid down in Article 35;

(c) where any of the processing operations referred to in paragraph 2 (a), (b), (c), (d), (e), (f), (g) or (h) exist, the controller or the processor acting on the controller's behalf shall carry out a data protection impact assessment pursuant to Article 33;

(d) where processing operations referred to in paragraph 2 (f) exist, the controller shall consult the data protection officer, or in case a data protection officer has not been appointed, the supervisory authority pursuant to Article 34.

4. The risk analysis shall be reviewed at the latest after one year, or immediately, if the nature, the scope or the purposes of the data processing operations change significantly. Where pursuant to paragraph 3 (c) the controller is not obliged to carry out a data protection impact assessment, the risk analysis shall be documented.