

15 July 2004

Dear Mr. Beales,

I am writing as the chairman of the Article 29 data protection working party (hereinafter “Article 29 Working Party”)<sup>1</sup> that was created in the European Union under the general data protection Directive<sup>2</sup>.

As you know, several issues have arisen recently concerning radio frequency identification (RFID) technology. It has come to our attention, in the context of the Workshop organised by the FTC on RFID technology on June 21<sup>st</sup>, that it was queried whether the above data protection Directive would apply to the collection and further processing of data through RFID technology. It appears that there was no consensus among the participants as to the answer.

In light of this uncertainty, I am therefore writing to clarify the application of the data protection Directive to the gathering and further processing of data through RFID technology.

In terms of scope, the data protection Directive applies to the processing of all personal data. Under the Directive, ‘personal data’ is very broadly defined and includes ‘*any information relating to an identified or identifiable natural person*’. It may then be asked whether this means that the data protection Directive necessarily applies to the collection of data through RFID technology. It is not possible to answer this question in the abstract. The answer will depend on the specific concrete application of RFID technology, particularly on whether the specific RFID application entails the processing of personal data as defined by the Directive.

In assessing whether the collection of personal data through a specific application of RFID is covered by the data protection Directive, one would need to consider whether the data collected through RFID technology *relates to an identified or identifiable natural person*. In carrying out such an assessment, it would be useful to take into account Recital 26 of the data protection Directive, which establishes that, to determine whether a person is identifiable, “*account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*”.

---

<sup>1</sup> Working Party 29 formally, Working Party on the protection of individuals with regard to the processing of private data, is an independent body set up by Directive 95/46/EC of 24 October on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of the Directive 2002/58/EC of 12 July concerning the processing of personal data and the protection of privacy in the electronic communications sector. Among others, such tasks including the interpretation of the provisions of the data protection Directive. It carries out this task by issuing recommendations, opinions and working documents on different aspects of the data protection Directive. Working Party 29 is composed of representatives of national data protection authorities of the EU Member States, by the European Data Protection Supervisor and by a member of the European Commission.

<sup>2</sup> Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In light of the above, while it is obvious that not all data collection by RFID technology will fall within the scope of the data protection Directive, it is also evident that there may be many scenarios where personal information is collected through RFID technology, the processing of which is covered by the data protection Directive.

Perhaps it may be useful here to give some examples of cases where the use of RFID technology clearly entails the collection and processing of personal data and consequent application of the data protection Directive.

As a first example, consider where a manufacturer of pharmaceutical products puts tags on a series of medicines which are sold upon presentation of a prescription. When the consumer buys the medicine, the information regarding the individual, the type of medicine bought, the time of the day, are entered into a database. If the individual returns for a refill, the retailer reader immediately identifies him/her. The information about the refill is logged and his/her behaviour in-store is monitored.

As a second example, consider where a conference organiser decides to tag conference badges which are delivered to delegates upon arrival and registration for a conference. RFID readers are placed in different parts of the conference premises. This allows the conference organiser to collect data regarding the location and movement of the conference participants. The data is linked to each participant and entered into a database.

In both the above scenarios, the provisions of the data protection Directive would apply. Among others, the relevant data controller/s for data gathered through RFID technology would be under an obligation to notify individuals of the collection, including the purposes for which the data would be used, of the legal grounds to collect such data (usually the individuals' consent) and of the rights of access and deletion as defined under the Directive.

I hope in this brief explanatory letter I have managed to sketch out a little of the complexity of the potential application of the Directive as well as the kinds of issues that are relevant to the determination of whether the EU data protection Directive is applicable to RFID technology. I expect to return to the subject in greater depth as the Article 29 Working Party is currently in the process of drafting a paper that will address the privacy implications of RFID technology.

Yours sincerely

Peter Schaar  
The Article 29 Working Party Chairman