

## Bijlage 1

## Summary

The development of Radio Frequency Identification – RFID – has been rapidly gaining momentum in recent times. The technology makes it possible to generate, store or otherwise process unprecedentedly large quantities of data, including personal data.

RFID has considerable implications for privacy and the perception of privacy, making it a subject of social debate. Cooperation and knowledge-sharing are very important in the formation of opinion on the social preconditions for the responsible use of RFID. In its specific role as a regulator, the Dutch Data Protection Authority [College bescherming persoonsgegevens (CBP)] is issuing this discussion document in order to further stimulate debate about the benefits and drawbacks of the technology.

### Privacy by Design

The main driving force behind the current use of RFID is improving logistics. The main drawbacks lie in the fact that the data obtained can be used to assess people, often without their knowledge. The most important guarantee to avoid or alleviate these risks must be sought in Privacy by Design. When designing applications and infrastructures, privacy risks must be taken into account from the outset.

### Other guarantees

Insofar as RFID applications involve personal data, the existing legal framework applies. However, there are also some grey areas in which it might become necessary to clarify or elaborate standards.

The development of new restrictive measures at too early a stage may stifle innovations, yet if such measures are taken too late, the social detriment may become irreversible. Given the speed at which RFID is developing, if balanced viewpoints on the use of the technology are to be formed it seems wise at this stage to place the emphasis mainly on the possibilities that Privacy by Design can offer for building in guarantees of responsible application.

### Awareness

All spheres of society need to be aware of the obligations, rights and possibilities applicable to them in environments in which RFID is used.

- *The people affected*

The people affected – citizens, consumers – can contribute, in organised fashion or otherwise, to social discourse about RFID. They have the right to information on the application of the technology, for example as a result of the clear and complete labelling of goods. Where possible, the people affected must have the option of renouncing the use of RFID to process data about them. Moreover they must also be able to view the data stored about them using RFID and have recourse to a good complaints resolution system for potential abuses or improper use.

- *The parties applying the technology*

If it is not sufficiently evident that the use of RFID carries privacy risks, it is advisable not to use it. It is not always appropriate to switch to a new technology. The use of RFID must be visible and transparent, proportional and safe. This aim may be served by collaborative projects to develop codes of conduct and best practices and to conduct audits. The provision of information to the public is essential.

We must guard against the accumulation of data acquired using RFID.

Finally, we must avoid the situation wherein the costs associated with counterbalancing RFID-related risks would have to be passed on to the people affected. These people must not, for instance, be penalized with higher prices or longer waiting times if they choose RFID-free alternatives.

- *The government*

Government authorities must not be focused on using RFID solely to be able to have ever more data at their disposal. Citizens must have confidence that the government is using RFID in a responsible way. As a special user of the technology, the government must assure itself of

optimum security facilities in a number of areas. It also has a role in stimulating the sharing of knowledge and research, both nationally and internationally, and in public information.

- *System developers*

System developers and designers of ICT tools must test RFID applications not just for their technical aspects, but also for their ability to ensure compliance with privacy regulations.

Technology-based measures are usually the preferred option for containing risk.