# Reputation Systems and Data Protection Law[1]

Tobias MAHLER, Thomas OLSEN

**Abstract:** Reputation systems can be used to provide relevant information about others when we interact with persons we do not know. However, reputation systems are challenged by concerns about privacy and data quality. This paper assesses how data protection law affects the design and the operation of reputation systems.

## 1. Introduction

Reputation systems collect information about a person or other entity (hereinafter "reputation subject") in order to evaluate the reputation subject's conduct and make this evaluation accessible for other users' decisions. An example is when Internet marketplaces like eBay* and Amazon.com* enable users to provide feedback on other users. In this case, feedback ratings are based on a user's past transactions and help other users learn about the transaction partner they are dealing with. Other examples include credit reporting services, which collect information about an entity's economic behaviour. This information is communicated e.g. to banks when they decide about credit. The latter kind of reputation systems has existed for a long time, but recent developments with respect to Internet based transactions have led to an increased need for reputation systems for this context.

Reputation systems may be of particular value when there is uncertainty about another person or entity involved in a planned transaction that involves risk. Transactions on the Internet involve a number of uncertainties with regard to the identity of the transaction partner, his or her ability and willingness to perform and the availability of realistic means of enforcement. The lack of experiences, knowledge or information about the other person or entity may lead us to refrain from the interaction. Reputation systems can provide us with relevant experiences others have had with this person or entity. Research indicates that reputation systems can encourage market actors to participate in transactions [1]. Reputation systems have also been considered as a compensation or supplement for lacking realistic means of enforcement on the Internet [2, 3, 4]. Thus, it is possible to think of new application scenarios for reputation systems, e.g. within virtual communities. The possibilities offered by reputation systems are promising, but one should also pay attention to possible threats.

---

[1] This paper was originally prepared for the eChallenges conference, Vienna 27-29 October 2004, and is published in the proceedings of the conference and in the book P. Cunningham & M. Cunningham (eds.), eAdoption and the Knowledge Economy: Issues, Applications, Case Studies, part 1, ISBN 1 58603 470 7, IOS Press, Amsterdam 2004, pp. 180-187. The research work has been partly financed by the European Commission through the project TrustCoM (A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations) and partly financed by the Norwegian Research Council through the project Personalised Internet-Based Services and Privacy Protection – PerProt.

## 2. Objectives and Methodology

The objectives of this paper are to investigate privacy and data protection problems related to reputation services. Introducing a reputation system requires a rather extensive collection, evaluation and disclosure of data. When deciding whether or not to participate in a reputation system, a potential user's concern may be whether the system will meet reasonable expectations with respect to privacy. Users may fear that too much information about them is collected and disseminated. There may also be concerns with regard to the "judging function" of a reputation system, where a user's conduct is evaluated. Such evaluations may be significant, since they are meant to be the basis for future decisions concerning him or her. This may raise questions with regard to how the user can dispute an evaluation he or she disagrees with. The lack of transparency and comprehensibility may increase these concerns. All these privacy-related concerns and fears may weaken the acceptance of a reputation system by potential participants.

Privacy concerns are not the only factors that can mitigate the uptake of a reputation system. From the perspective of the entity that uses the reputation profiles for decisions, the relevance and accuracy of the reputation data is essential. This decision-maker is interested in optimized data quality and has a separate interest in the quality of the process that generates reputation profiles. If the quality is not satisfying from this perspective, this may weaken the value and utilization of the reputation system.

Data protection law provides rules that secure a fair processing of personal data. Furthermore, data protection law aims at enhancing data quality and contributes to increased transparency with respect to how data is processed. Therefore, data protection law can contribute to improve the value, acceptance and uptake of reputation systems.

The aim of this paper is to provide guidelines for the design of reputation systems from a data protection perspective. It identifies legal and technical issues that should be addressed in order to design lawful and legitimate reputation systems. We will not analyse a specific reputation system, but rather explore different possibilities when developing a reputation system. Technical and organisational design choices may have legal consequences, particularly with respect to data protection law.

## 3. Data Protection Law

In Europe, data protection is subject to a rather strict legislation both on the European and national level. In this respect, reference will be made to the EC Directive on Data Protection (hereinafter EC Directive [5]) and its implementations in relevant national acts on privacy and data protection. A reputation service dealing with personal data is bound to follow the applicable national data protection law.

### *3.1 Who is Who in Data Protection Law*

This section will introduce the central actors and terms used in this paper to analyse reputation systems in the light of data protection law.

Personal data: This term is defined in the EC Directive, Article 2, as "any information relating to an identified or identifiable natural person". "Any information" is a rather wide wording, which includes everything that can be perceived, sensed or registered etc. about a person. There are reasonable arguments to hold that also opinions, even false ones, must be qualified as personal data [6]. An "identifiable person" is one who can be identified, "directly or indirectly". Some of the data processed by reputation systems can be personal data. However, the data will only fall into this category, if the data subject is a "natural person".

Data subject: In data protection law, the data subject is the natural person (individual) to whom the personal data refers. However, reputation systems may also hold data that refers to other entities than individuals. We will therefore introduce the term “reputation subject”.

Reputation subject: A reputation system can in principle administrate the reputation of individuals, groups, organisations, collective entities (may be legal persons). This paper does not deal with objects in reputation systems. We will use the term reputation subject when referring to the entity to which the reputation data relates. In principle, reputation systems must only comply with data protection law when processing data on individuals. Other entities protection is usually limited to laws dealing with defamation, breach of confidentiality and unfair competition. This is in contrast to data protection law, which e.g. ensures data quality, i.e. that data are relevant, correct, complete and not misleading in relation to the purposes for which they are processed. Arguably, collective entities and individuals share some interests, particularly with respect to the quality of data [7]. Therefore, reputation system providers may want to choose to follow central data protection rules also when processing data on other reputation subjects.

Data controller: In the EC Directive, the data controller is defined as anybody who determines the purposes and means of the processing of personal data. When deciding who is a data controller in a reputation system, one has to identify the person or organisation with decision making power. If the system is developed by one entity but independently used by another, the latter is the data controller, since this entity determines the purposes and means of the processing. In principle, it is not impossible to think of more than one data controller. Data controllers are responsible for the lawful processing and may be held liable.

### *3.2 Basic Principles*

The most important rules in data protection law can be expressed in relation to a number of basic principles [8] to be found in most international and national data protection instruments and laws.

- Fair and lawful processing: Personal data must be processed fairly and lawfully.
- Purpose specification: Personal data must be collected for specified, explicit and legitimate purposes and not further processed for other purposes.
- “Minimality”: The collection and storage of personal data should be limited to the amount necessary to achieve the purpose(s).
- Information quality: Personal data should be valid with respect to what they are intended to describe and relevant and complete with respect to the specified purpose(s).
- Data subject participation and control: Persons should be able to participate in the processing of data on them and they should have some measure of influence over the processing.
- Limitation of fully automated decisions: Fully automated assessments of a person’s character should not form the sole basis of a decision that impinges upon the person’s interest.
- Disclosure limitation: The data controllers’ disclosure of personal data to third parties shall be restricted, it may only occur upon certain conditions.
- Information security: The data controller must ensure that personal data is not subject to unauthorised access, alteration, destruction or disclosure.
- Sensitivity: Processing certain categories of especially sensitive data is subject to a stricter control than other personal data.

## 4. Data Protection Law and Reputation Systems

In this section, we will correlate these principles of data protection law with some of the possible characteristics of reputation systems. When designing a reputation system, one is confronted with a number of technical and organisational choices. These choices have an impact on how the reputation system processes personal data.

### *4.1 Participation in Reputation Systems*

The principle of fair and lawful processing generally requires data controllers to take account of the interests and reasonable expectations of data subjects. This also implies that data subjects should not be unduly pressured into participation in reputation schemes. The principle of fair and lawful processing is embodied in a number of requirements in data protection law. The data subject's consent is the most important criterion to make processing of personal information in reputation systems lawful. The EC Directive defines the data subject's consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Articles 2 (h) and 7). The Directive requires timely and comprehensible information to be provided to the data subject, and the consent should be expressed through a freely and positive action. One should note that the processing of personal data also may be lawful without consent if other criteria are fulfilled. This may be the case, e.g. if the data controller's interest overrides the privacy interest of the data subject, or if the processing is necessary in relation to a contract or a legal obligation (Article 7(b), (c) and (f)).

When implementing a reputation system, one may consider making it mandatory to achieve maximum participation and value of the system. Most auction sites have a mandatory reputation system where participation in the reputation system is a condition for using the services. A discretionary/optional reputation system might be an alternative to be considered, even though this may cause some practical disadvantages.

### *4.2 Centralised and Distributed Reputation Systems*

The current reputation systems that have seen some form of deployment are centralised in the meaning that there is one centralised reputation service provider. For example in Amazon.com, information is centrally administrated.

This can be compared to distributed reputation systems, where every entity runs a local instance of the reputation system. Also hybrid systems have been suggested, combining elements characteristic for centralised and distributed reputation systems [9]. One advantage with a distributed reputation system from a data protection perspective could be that information is spread between all participants, thus hindering accumulation of information in one place. Even in a fully distributed system, the system designer should ensure that relevant data protection principles are respected, including the right to access own personal data and the possibility to rectify false sets of data. In some cases it may be difficult to identify the data controller(s) in distributed systems.

Obreiter has suggested the use of so-called "evidences" in distributed reputation systems [10]. These non-repudiable tokens describe the behaviour of a specific entity in a statement. Digital signatures are used to make sure that the statement can be passed on to others. For example one party in a transaction can pass an evidence token to the other party, declaring the receipt of the item they trade. This receipt can later be used in order to document the behaviour, i.e. that the item has been sent and was received. In a data protection perspective, the use of such tokens has the advantage that they are not controlled by a central instance, but by the data subject himself. However, if the statements are too

detailed and the data subject is expected to transfer many such tokens in order to document trustworthiness, this could lead to an excessive dissemination of personal information.

### *4.3 Identity and Identification*

Reputation subjects may participate in a reputation system disclosing their real life identity to the other participants, or they may act under a pseudonym. From a data protection point of view, this choice is one of the most fundamental issues. One has to consider the necessary functionality of the reputation system and should be aware of technical, organisational and legal means to protect the identities and the personal data of the users.

"Personal data" is defined in the EC Directive, Article 2, as "any information relating to an identified or identifiable natural person". An "identifiable person" is one who can be identified, "directly or indirectly" within a reasonable time, considering the necessary effort taking account of all the means likely reasonably to be used. Existing reputation systems often use pseudonyms to hide the identities of the users. We are not aware of fully anonymous reputation systems. In eBay for example, users register their contact information and are provided with a pseudonym which is used for transactions on the marketplace. Since the person behind the pseudonym can be identified, the pseudonym itself and data related to the pseudonym are personal data in relation to the EC Directive. It is possible to think of "strong" or "weak" pseudonyms in relation to how difficult it is to reveal the real-world identity for other users of the reputation system [11].The disclosure limitation principle provides that strong pseudonyms should be preferred to weaker ones.

When issuing a pseudonym, the reputation system has different possibilities to verify the identity of the person. If a strict verification procedure is implemented, this strengthens the possibilities of holding the user of a pseudonym liable for misconduct. Pseudonyms that are linked to a verified identity may be trusted more easily. It is also possible to think of reputation systems where parties could participate under different pseudonyms depending on the need for assurance and reliability [12]. If a reputation system allows the use of multiple pseudonyms, these should not be linked to one common reputation profile [13].

Reputation systems should be limited to a specific marketplace or environment. A general reputation service that covers all kinds of actions in different contexts may lead to an excessive disclosure of personal information. Therefore, one should be careful with linking profiles from different reputation systems.

### *4.4 Types of Data in Reputation Profiles*

A reputation system can generate a reputation profile by combining elements of evaluation ("excellent eBay buyer") with more factual elements regarding e.g. the timeliness of the transaction, its value or category. In this context, fact and evaluation are not seen as two dichotomist categories. This is rather a question of degree. For example, the comment "timely delivery" may include elements of both facts (delivery date) and evaluation (relation of the delivery date to rules about delivery, e.g. in a contract).

Some reputation systems, e.g. within credit rating, are based fully or mainly on factual information. Facts can either be made available to the end-user as separate information in order to provide a more comprehensive picture of the reputation subject, or they can be combined with the evaluation. The reputation system can collect factual information from a party's declaration, or simply track some of the information that is processed in relation to a transaction. Any collection from the data subject must be done in a fair and lawful way. This may require an informed consent, i.e. the participant must fully understand what is being tracked and for what purposes the data will be used. Ideally this should be explained both in a detailed way and in a way that is understandable for the average participant. This must be done *prior* to the collection of information.

The other element in reputation systems consists of evaluations, normally provided by other participants. In a data protection context, this is classified as the collection of personal data from third parties. The reputation system must additionally ensure that the data subject is informed about the fact that personal data is collected from others. Evaluations may be thought of as rather uncomforting by the reputation subject, since this can be perceived as a judgment about him or her. Two data protection principles can assist the reputation subject in such situations: The principle of data quality and the principle of the data subject's participation and control. Both principles are reflected in Art. 12 (b) of the EC Directive, according to which the data subject has a right to have incomplete or inaccurate data rectified, erased or blocked. Obviously, evaluations made by third parties are difficult to verify for reputation systems. To cope with this problem, some reputation systems allow participants to cross-comment evaluations. Interestingly, research has shown that this function in eBay's feedback system leads to an under-reporting of negative comments because of the fear for negative cross-comments [14]. However, while minor problems are under-reported, participants do report instances of fraud, which indicates that the system seems to work best when it is most needed [15].

### *4.5 Generation of Reputation Profiles*

Reputation profiles can be generated by aggregating factual elements and evaluations. This can result in some kind of score, e.g. a number of stars (Amazon.com) to be communicated to other users. According to the EC Directive, Article 12 (a), the data subject has a right to access the "knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions". Automatic decisions based on reputation profiles will be discussed below in section 4.7. However, we can already state that this may require that reputation systems have to inform the data subjects about the algorithm that is used to generate the reputation profile. Additionally, the algorithm has to comply with the principle of information quality in the sense that it generates information that is relevant, adequate and not excessive in relation to the purpose of the processing.

### *4.6 Access to and Disclosure of Reputation Data*

Any data subject has a general access right to data on himself or herself (Art. 12). In the sequel, we will explore the limitations with respect to the disclosure of data to third parties.

Access to reputation data by third parties must be dealt with in light of the disclosure limitation principle. According to this principle, the data controller's disclosure of personal data to third parties shall be restricted, it may only occur upon certain conditions. The data subject may consent to such disclosure. Reputation data may be accessible all the time for any interested party, for example on a web site. Alternatively, access may only be given individually upon request.

When designing a reputation system, one should have in mind that some types of data are more sensitive than others. The EC Directive contains a catalogue of categories of especially sensitive data, which for example includes data concerning health or sex-life (Article 8.1.). This kind of data can only be processed under certain conditions. A reputation service that deals with data categories contained in this catalogue must restrict the disclosure to certain cases instead of allowing everybody to access the reputation data. Additionally, also other categories of personal data may have a strong impact or importance for a person, even though the category is not included in this catalogue. The sensitivity of personal data depends on its context. One example could be a person's credit history when applying for a credit. The importance of this type of data has led to special rules in some countries, even though financial information is not classified as sensitive.

In this respect, reference should be made to the rules about credit reports under Norwegian [16] and Swedish law [17]. These rules regulate the disclosure of credit information by professional actors who specialise on trading such data. For example, disclosure of credit information is only allowed if the requestor has a legitimate interest in receiving the data. Additionally, every time the recorded information about an individual is disclosed upon request, the credit information service has to contact this person (normally by letter). The data subject must be informed that data has been disclosed upon request, who has requested it and what has been communicated. Here, also legal persons are provided rights of access to information. This is one of the few examples where data protection law extends its scope to others than individuals.

The rules on credit reporting are the only set of rules that specifically regulates some reputation systems. However, it applies only to credit agencies. Other reputation services are not (yet) subject to specific regulation. Nevertheless, the main safeguards and procedures could be used analogously in other contexts where a reputation system deals with sensitive information. Reputation systems should consider following some of these procedures in order to ensure the acceptance of their system.

### *4.7 Decisions Based on Reputation Profiles*

The major aim of reputation systems is to provide a basis for well-informed future decisions. In the cases of eBay and Amazon.com, the decision is whether or not to trust a certain pseudonym in the online market place. Decisions related to other reputation systems could include whether or not to participate with a subject in a virtual organisation, whether or not to allow a member of a virtual community access to a certain resource, whether or not to avail a credit to a person etc. There are basically two ways how these decisions can be made. Either the decision maker decides freely and uses the registered reputation as one of the premises for a decision. Alternatively, the decision can be made automatically on the basis of the calculated reputation score. Automatic decisions are considered as problematic in a data protection perspective, and there are special rules for such decisions.

Article 15 limits the use of certain automatic decisions based solely on automatic processing of data [18]. This applies only to decisions that are legally binding or which significantly affect the data subject. The data processed must be intended to evaluate certain personal aspects of the person who is targeted by the decision. These personal aspects include performance at work, creditworthiness, reliability, conduct etc, which all are aspects that could be evaluated in a reputation system. As mentioned above in section 4.5, the data subject has a right to be informed about the logic involved in any automatic processing of data concerning him or her (Article 12 (a)). The data subject may also object to an automated decision and require a decision by a human (Article 15 (1), exceptions in (2)). Hence, when opening for automatic decisions based on reputation scores, one should be aware of these restrictions as implemented in national law.

## 5. Concluding Remarks

Reputation systems should be carefully designed in order to comply with data protection law, if they (at least in part) deal with personal data. This will ensure a fair administration of information and users will more easily accept to participate in the reputation system. The above mentioned basic data protection principles can also be considered as a means to improve the data quality in a reputation system, which makes the reputation system more relevant as a basis for a decision and more attractive for the end-user. Below, we have tried to capture some relevant factors that should be considered to ensure that reputation systems respect data protection law.

- Participation in a reputation system should be limited to actors who have expressed their well-informed consent.
- The purpose(s) of the reputation system should be clearly defined.
- The collection, storage and dissemination of (personal) data should be limited to the amount necessary to achieve the purpose(s).
- The procedures regarding the collection and evaluation of personal data should be transparent and communicated in a comprehensible way.
- Reputation subjects should be allowed some participation and control with respect to the collection of data about them and with regard to the generation of their reputation profile.
- The quality of both the collected data and of the aggregated reputation profile should be valid with respect to what they are intended to describe and relevant and not incomplete with respect to the specified purpose(s).
- Fully automated decisions on the basis of reputation profiles should be avoided. If they are chosen, there should be full transparency regarding the algorithms used to calculate the reputation score and to make the decision. Additionally, the data subject should be able to claim a human decision.
- The security of (personal) data must be ensured.
- Reputation systems that deal with sensitive data should use a stricter policy to protect personal data.

These recommendations may assist in identifying legal problems, indicating that the reputation system developer and the data controller should seek legal advice to clarify how the law in the relevant jurisdiction solves these issues. The recommendations may also be used as a point of departure for future research on reputation systems with regard to data protection law.

## References


* Trademark or registered trademark of eBay Inc., Amazon.com Inc. and PEZ Candy Inc.

[1] Keser, C., Experimental games for the design of reputation management systems, IBM Systems Journal, Vol. 42, No. 3, 2003, pp. 498–506.

[2] Friedman, D., Contracts in Cyberspace, available at http://www.daviddfriedman.com/Academic/contracts_in_%20cyberspace/contracts_in_cyberspace.htm, last visited 23 April 2004.

[3] Gilette, C.P., Reputation and Intermediaries in Electronic Commerce, Louisiana Law Review, Summer 2002, pp. 1165–1197.

[4] Block-Lieb, S., E-Reputation: Building Trust in Electronic Commerce, Louisiana Law Review, Summer 2002, pp. 1199–1219.

[5] Directive 95/46/EC, Official Journal L281, 23/11/1995 pp. 31–50.

[6] Bygrave, L., Data Protection Law, Approaching Its Rationale, Logic and Limits, Kluwer Law International, The Hague, London, New York, 2002, p. 46.

[7] Bygrave, supra note 6, chapter 12.

[8] Bygrave, supra note 6, pp. 57–68 and 2.

[9] Fernandes, A. Kotsovinos, E., Östring, S. Dragovic, B., Pinocchio: Incentives for Honest Participation in Distributed Trust Management, in Trust Management, Second International Conference, iTrust 2004, LNCS 2295, pp. 63–77.

[10] Obreiter, P., A case for Evidence-Aware Distributed Reputation Systems, Trust Management, supra note 9, pp. 33–47, p. 39.

[11] Clarke, R., Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice, http://www.anu.edu.au/people/Roger.Clarcke/DV/UIPP99EA.html, last visited 29 April 2004.

[12] See for example the RAPID-project, Roadmap for Advanced Research in Privacy and Identity Management, http://www.ra-pid.org/, last visited 29 April 2004.

[13] See also Seigneur, J.-M and Jensen, C. D., Trading Privacy for Trust, Trust Management, supra note 9, pp. 93–107.
[14] Gilette, supra note 3, p. 1191.
[15] Block-Lieb, S., supra note 4.
[16] Norwegian regulation on the processing of personal data, Forskrift om behandling av personopplysninger (personopplysningsforskriften) section 4.
[17] Sweden's Credit-Reporting Act, Kreditupplysningslag (SFS 1973:1173).
[18] For more details about Art. 15 refer to Bygrave, L., Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling, Computer Law & Security Report, 2001, volume 17, pp. 17–24.