“Tap and Pay”: Who’s Looking After Your Privacy?

Privacy aspects of contactless payments viewed in connection with Dutch law

Using your smartphone or cash card to “tap and pay” contactless for goods and services is a great convenience. Contactless payment is available in more than 50 countries of the world and necessitates handling consumers’ personal data. The article first explains what contactless payment is (I) and outlines the battle between Near Field Communication (NFC) and Quick Response (QR) for the technological standard (II). Then the legal framework for the protection of personal data is analysed for each player participating in the data processing chain (III.) and rounded up with a list of key privacy obligations (IV.).

I. What is Contactless Payment?

If you’re going out for the evening – dinner and a good film, for example, plus parking fees – how are you going to pay for it? You can obviously pay cash or by PIN. But there are an increasing number of places nowadays where you can also “tap and pay” using your smartphone or cash card. This means holding your smartphone or cash card against the payment terminal just for a second. It’s a simple way of paying smaller or bigger amounts alike. The tap-and-pay method is quick and practical. And it will soon be possible to read out your loyalty cards at the same time too – so no more messing about looking for each individual loyalty card in your wallet.

“Tap and Pay”, “Wave and Pay”, “swiping” or “mobile payment” – these are all names for the new payment method. Technically speaking, “contactless payment” is really the most appropriate name. For small amounts, you don’t usually even need to key in your PIN code. This means that contactless payment transactions are easily 7 seconds, or 40 % quicker. It also means that the average supermarket can save up to 4 hours a day on its staff. Fewer employees means lower costs, while customers can be served faster without needing to carry as many cash cards or as much money around with them. As far as shops are concerned, the efficiency and ease of use can also encourage impulse buying, which is good for business.

1. Parties Involved

A number of parties are involved in contactless payments. First of all, of course, the shopkeepers, who are also known as “the Merchants”. Secondly, there are the banks that facilitate the payment transactions. These include your own bank (the issuing bank) and the shopkeeper’s bank (the acquiring bank). Other major parties include providers of payment terminals and the relevant services (payment service providers). And if you use your smartphone to pay, this will involve your telecom provider (Mobile Network Operator, MNO), your telephone supplier, and developers of apps as well.

These parties must be in possession of your personal data – such as your transaction details – in order to facilitate payment transactions, but they can also access data on your location or on your favourite products, for example. This personal data is of tremendous value to companies. And if the data can be combined and analysed, companies can create customer profiles and send you targeted offers. However, they will still have to abide by the privacy regulations, which are becoming increasingly stringent.

2. Global Spread

This innovative payment method is available in more than 50 countries all over the world, 34 of which are in Europe. Remarkably, Poland leads the field in this respect: 33 % of all payments made in this country have now been replaced by contactless transactions.

The Netherlands is not an early adopter openly embracing contactless payments. The new method was examined in the Netherlands by carrying out a large-scale test in 2013 entitled “Paying by mobile phone in Leiden”. Around 1,000 consumers and 150 businesses including supermarkets, department stores and catering establishments took part in this test, which was devised by ABN Amro, ING Bank and Rabobank in collaboration with MasterCard, KPN and the municipality of Leiden. The results of the test were positive: 78 % of the consumers...
were very happy with the fact that contactless payment was so easy and convenient.\(^2\)

Meanwhile, several Dutch banks have introduced further developments in contactless payment using a cash card, while other banks are also focusing on payments using a smartphone with NFC technology.\(^3\)

More than 30,000 payment terminals in various Dutch towns and cities have now been adapted for contactless payments. These terminals are located in places where many transactions are effected within a short period of time, such as Schiphol Airport and railway stations. Some chain stores like Blokker (a large chain for household supplies) have already adapted their payment terminals for contactless payments, while H&M and IKEA are due to introduce contactless payment terminals by the end of 2014.

II. Battle for the Technological Standard

With respect to technology, two different types are especially popular in connection with contactless payment: Near Field Communication (NFC) and Quick Response (QR).

1. Near Field Communication

NFC technology has been used in various sectors in the Netherlands since 2000, including the home care sector. Moreover, many consumers will already be familiar with this technology due to the new public transport pass. NFC is a variation on Radio Frequency Identification (RFID) technology, a kind of barcode that uses radio waves. But NFC technology can do much more than merely read data for processing payment orders: it can also be used for reading loyalty cards, gift vouchers, special discount offers and other services.

If you want to use NFC technology to pay by smartphone, your phone must have an NFC chip. This can be integrated into the phone or be affixed to it with a sticker and combined with an appropriate SIM card. You may still need a PIN code, especially when paying larger amounts. You can key in this PIN code on your smartphone beforehand, so that all you need to do in the shop is confirm payment. In addition, you can install a “wallet app” (known simply as a “wallet”) on your smartphone, which functions as a sort of electronic purse. You can keep your loyalty cards and credit notes in this wallet as well as your cash card. You can even carry out small and simple transactions that don’t use a wallet if your smartphone is turned off or if it needs recharging.

You can see whether this type of contactless technology has been incorporated into your cash card from the small icon on the front of the card.\(^4\) Again, you may occasionally have to key in your PIN code, depending on the amount you’re paying, which bank you have and also on the settings of your card.

2. Quick Response

The Quick Response (QR) code, in black and white squares, has also been increasingly used for payment transactions since 2011. You can use the QR code to make payments with your smartphone via a payment app, without requiring a separate chip. The advantage for shopkeepers is that they don’t have to adjust their payment terminals. All you have to do is display the code clearly on the invoice, for example, so that it can be scanned.

3. And the Winner is ...

The type of technology that will eventually become the standard depends on the parties concerned. At present, it seems as if most of the market parties in the Netherlands have decided in favour of NFC technology, although the QR code is gaining popularity too.

Cash cards issued by ABN Amro and ING are equipped with contactless technology. The latest smartphones manufactured by Samsung, HTC, Nokia and others have an NFC chip, while the Android operating system is also geared to NFC technology. In September 2014, Apple announced that it entrusted its Apple Watch and iPhone 6 with the NFC technology, enabling their feature Apple Pay.

These practical examples show that more than one technological road leads to Rome. In view of the fact that NFC technology currently seems to be the most popular, this article will focus on the use of this type of contactless payment by smartphone. However, the privacy aspects discussed here are equally important with respect to applications using the QR code and other technology.

III. Legal Framework – Protection of Personal Data

Besides technology, observing due care when handling consumers’ personal data will be crucial for the considerable increase anticipated in contactless payments.\(^5\) Any party that processes personal data must comply with the applicable national data protection rules. In the Netherlands, the 1995 EU Privacy Directive (95/46/EC) was implemented in the Dutch Data Protection Act (Wet bescherming persoonsgegevens).\(^6\)


\(^{4}\) Strictly speaking, NFC technology is not used when using a cash card to make contactless payments.

\(^{5}\) On 17 June 2014 the Italian Data Protection Authority issued a Resolution (Doc. 3203981) providing rules for the processing of personal data within the context of contactless payments. See: http://www.italiancomplianceforum.com/wp/97.

\(^{6}\) Act dated 6 July 2000 and containing regulations pertaining to the protection of personal data (Personal Data Protection Act), and European Parliament and Council Directive 95/46/EC dated 24 October 1995 and pertaining to the protection of natural persons in connection with per-
Important interpretations of certain terms contained in the Directive (and the national data protection acts) can be found in the opinions and recommendations given by the Article 29 Working Party, the European Commission’s independent advisory body for privacy-related matters. This working group has not yet given a specific opinion on contactless payment. Nevertheless, various opinions are available with respect to general privacy-related matters which are also relevant to the privacy requirements for contactless payment. These include opinions on the following terms: “personal data”, “anonymisation techniques”, “geolocation services” and “purpose limitation”.7

Proposals at European level to replace the Privacy Directive with a General Data Protection Regulation are currently under discussion.8 If this Draft Data Protection Regulation passes, this would incorporate the privacy laws for all EU member states into one single European Data Protection Regulation, which will apply directly. This new Draft Data Protection Regulation is expected to entail greater privacy obligations, as well as substantially larger sanctions. According to current proposals, these may amount to as much as 5% of a company’s global annual turnover, or 100 million euros, whichever is greater. Companies would be well advised to examine ways in which they can anticipate the new obligations now.9

1. Personal Data and Processing Operations

Following on from the EU Privacy Directive, the Dutch Data Protection Act defines personal data as all data that can be directly or indirectly traced to a natural person (the data subject). With respect to contactless payment, this could be your bank account number, your phone number, or your smartphone’s MAC address (its unique code), but it could also be a combination of the information relating to your transaction, such as your location, the date, the products you purchase and the price you pay for them. Processing your personal data may be said to exist even if your name is not known, provided that the data or a combination of the data can be traced to you.10

When making contactless payments, processing your personal data starts as soon as you sign a mobile phone contract or open a current account. Your telecom provider or bank will then process your personal data. Another moment on which your data is processed is when your smartphone or cash card is enabled to make contactless payments. After this, data is processed when you actually make such payments. This generates a new data processing operation involving the shopkeeper, your bank and the telecom provider. Your personal data is also processed when tracing or identifying any fraud committed using your smartphone or cash card. And finally, your personal data can be processed for marketing purposes or for fulfilling statutory obligations.

All these data processing operations must comply with general privacy principles, i.e. the requirements of data minimisation, proportionality and subsidiarity. These requirements inter alia follow from articles 6, 7 and 9 of the Dutch Data Protection Act and Consideration 28 and article 6 of the Privacy Directive. These general principles can furthermore be derived from the Draft Data Protection Regulation, in particular in Consideration 30 and article 5.

The data minimisation requirement means that no more data may be processed than is necessary for the purpose for which the data is compiled. The proportionality requirement means that the data subject’s interests must be taken into consideration. It also means that curtailment of the data subject’s interests may not be disproportionate in relation to the purpose served by processing the data. And finally, the subsidiarity requirement means that if the same purpose can be attained using other and less radical means, such means must then be used. The three principles are further elaborated below in connection with the (legitimate) purposes and the legitimate bases of the data processing.

2. Data Controllers and Data Processors

Pursuant to article 1 of the Dutch Data Protection Act, the parties involved in contactless payments should be qualified either as “data controllers” or as “data processors” in order to be able to determine which privacy obligations each party must fulfil. The definitions of data processor and data controller originate from article 2 (d and e) of the Privacy Directive, which definitions have been implemented in article 1 (d and e) of the Dutch Data Protection Act. Similar wording is used in the Draft Data Protection Regulation. See also Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 17 February 2010.

a) Data Controller

The major privacy obligations lie with the data controller. This is the party that determines the purposes and the means with respect to data processing. A number of data controllers will be involved in contactless payment, each of which processes personal data for their own ends. It is likely that differentiated responsibility will exist in this respect, meaning that each party is independently responsible for its own part of the data processing. As far as the data subject is concerned, it means that he can address each data controller on that part of the data processing for which the party in question is responsible. The division of roles between the parties involved in contactless payment will eventually emerge from the agree-

8 See: http://ec.europa.eu/justice/data-protection/. EU member states have agreed to conclude negotiation regarding the EU Data Protection Draft Regulation in 2015. It is now looking like there is a real possibility the Draft Data Protection Regulation will be enacted in 2015 which, on the basis of the currently envisaged two year implementation period, would see it implemented in 2017.
9 For this article we have relied on the version of the Draft Data Protection Regulation that was adopted by the European Parliament on 12 March 2014 (European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).
10 The concept of personal data was subject of the EU Court of Justice decision of 17 July 2014. See cases C-141 – and C-372/12, YS v. Minister voor Immigratie, Integratie en Asiel. See also CRI 2014, pp. 138.
ments made between the parties and the way in which they have actually implemented them.

b) Data Processor
Unlike the data controller, the data processor processes personal data in accordance with instructions issued by the data controller, not for its own purposes. In this respect, the scope of such instructions may not exceed data processing that the data controller is allowed to carry out under the law. In addition, one party may be the data controller for one part of the data processing and the data processor for another part of it.

3. Purposes
Article 6 of the Dutch Data Protection Act states that all data must be processed in accordance with the law. Furthermore, data must be processed with all due care and attention and personal data may only be processed for legitimate purposes which are clearly and explicitly specified. This is also known as the purpose limitation principle, which is laid down in article 7 of the Dutch Data Processing Act, implementing article 6 (b) of the Privacy Directive. See further also article 5 (1) (b) of the Draft Data Protection Regulation.

Firstly, the purposes must be explicitly specified and secondly, in the event of further processing, they may not be incompatible with the purpose for which the data in question was originally compiled.

4. Parties, Purpose Limitation and Their Respective Roles
We have already cited a number of the parties involved in contactless payment in the foregoing. Further details of their roles or potential roles are given below whilst bearing the purposes of the data processing in mind.

a) Merchants
As a data controller, shopkeepers or merchants will process your data in order to carry out the transaction. The data over which shopkeepers have control includes a description of the transaction, the date and time of the transaction, the amount paid and your account number. The purposes for which shopkeepers process your personal data are the performance of the sales contract, handling the transaction and the relevant administration. We can also cite a number of secondary purposes such as improving their services or updating the product range, or direct marketing purposes.

b) Banks
Banks are also considered to be responsible as data controller for the data they process in connection with contactless payments. As in the case of shopkeepers, the primary purpose of data processing for banks is to carry out the sales transaction. There are also related purposes such as tracing and combating fraud, as well as making tailored offers.

An initiative on the part of ING was given extensive news coverage in the Netherlands in March 2014. Subject to consent, the bank was planning to use its account holders’ data to permit third parties to make offers. The Equens payment processor came up with a similar plan in 2013. Both these plans resulted in uproar and questions were even asked in the Dutch Parliament. ING and Equens decided to shelve their plans. Their ideas were not new and were potentially lucrative. The Bank of America has permitted third parties to offer clients advertisements on the basis of payment data since 2012. It has been estimated that this has since resulted in a profit of 180 million euros for the bank and a saving of 18.2 million euros for its clients.

Besides the Dutch Data Protection Act, banks will also have to abide by the Code of Conduct for the Processing of Personal Data by Financial Institutions with respect to privacy. This Code of Conduct is a sector-specific elaboration of the statutory provisions that apply to the processing of personal data.

c) Telecom Providers
If you make payments with your smartphone, it serves as a platform that is helpful for services provided by third parties such as your bank. As in the case of other apps you use on your smartphone, your telecom may play a facilitating role and provides the infrastructure to be used when sending data. Depending on the technique that is used, the telecom provider can act as a data processor.

Whether or not the telecom provider can also be considered a data controller will depend on the services or additional services it provides. If your smartphone uses NFC technology, your SIM card stores the application used to send data on behalf of this NFC technology. The telecom provider may have access to this and process data. It can also process personal data by providing an app that integrates a number of payment services. If the telecom provider provides these services itself as well as determining the purpose and the means to be used for the data processing, it is likely that it is also a data controller within the meaning of the Dutch Data Protection Act. The nature of the purposes depends on the services provided.

12 See for the ING project: Het Financieele Dagblad of 14 November 2014, “ING schuift commercieel uitbaten klantgedrag op lange baan”.
Telecom providers and banks or other financial institutions may engage Trusted Service Managers (TSMs) for the safe exchange of data among themselves. These TSMs act as intermediaries, and can ensure that the bank is able to access part of the application on the SIM card (Secure Element) on the instructions of a telecom provider. In some cases, the telecom provider’s TSM can also ensure that access is blocked if your smartphone is stolen. Since TSMs process personal data on behalf of the relevant bank or telecom provider, they are considered to be processors within the meaning of the Dutch Data Protection Act.

d) Payment Service Providers

It is conceivable that personal data is also processed if a third party provides the payment terminal plus the relevant software and services. These services are provided on behalf of the shopkeeper, and the payment terminal provider may exclusively process personal data on the shopkeeper’s instructions. Insofar as the payment terminal provider processes personal data, it is likely that it is a processor.

e) App Developers

You don’t need to use an app for contactless payments using NFC. However, you can download wallet apps that can link different cash cards and loyalty cards. If a bank or telecom provider has an app developed and administered in order to facilitate contactless payment, the developer is also a processor on behalf of the bank or telecom provider. Parties other than banks or telecom providers are currently developing wallet apps too. If these parties determine the purpose and the means for the processing themselves, they may be regarded as data controllers if, for example, they place targeted advertisements.

Google launched the Google Wallet app in the United States in 2011. This app enables consumers to pay in many shops in the United States by linking their credit cards, gift vouchers or loyalty cards to their accounts. Google’s revenue model lies in the advertisements shown to users, and the company may be regarded as a data controller or a data processor depending on how it develops the app further: as a platform for third-party cash cards or as a provider of its own services.

5. Justification Grounds

Besides purpose limitation, the Dutch Data Protection Act requires data processing to be based on one of the restrictive grounds for justification specified by law. The type of data processed and the purposes for which it is processed will determine which ground for justification will apply. The justification grounds as specified below are laid down in article 8 of the Dutch Data Protection Act, which implements article 7 of the Privacy Directive. See also article 6(1) of the Draft Data Protection Regulation.

a) Performance of the Contracts Concluded with You

First of all, a great deal of your personal data may be processed pursuant to the contracts you conclude with shopkeepers, your bank and your telecom provider respectively. For example, shopkeepers will be allowed to process your transaction data so that they can supply the goods you have bought from them. Secondly, your bank has undertaken to carry out your transactions and to do this, it needs to process your transaction data as well. And thirdly, you will also have to conclude a contract if you use services provided by your telecom provider or if you install an app, and some of your personal details may also be processed pursuant to this contract.

b) Legitimate Interests

Not all data processing carried out in connection with contactless payment can be traced to a contract concluded with you. In such cases, a different ground for justification will have to be put forward. If the data controller – the bank, for example – is able to demonstrate that processing your personal data is necessary to promote its own legitimate interests or those of a third party provided with this data, it is allowed to process your data. In this respect, however, the data controller must demonstrate that its own interests and/or those of the third party in question should be given priority over your privacy interests. This principle therefore requires the relevant legitimate interests to be balanced against each other, with both business and private interests playing a role here. For example, your personal data may be processed by invoking this ground for justification for the purpose of tracing and combating fraud.

c) Statutory Obligations

Banks and telecom providers are also allowed to process people’s personal data in order to fulfil their own statutory obligations. Examples of statutory obligations include tax-related obligations laid down in the Dutch Civil Code and tax legislations and more specific ones such as the telecom provider’s duty to report data leaks (see below). Furthermore, your telecom provider will also have to process and store your transaction data, at least for the time being, in order to comply with its obligation to retain data.

Pursuant to the EU Data Retention Directive, EU member states are obliged to ensure that certain parties – including telecom providers – keep Internet data available for use during a period of no less than 6 months and no more than 24 months in connection with prosecution, information and security. The retention obligation has been incorporated into the Telecommunications Act in the Netherlands. On 8 April 2014, however, the Court of Justice of the European Union declared the Data Retention Directive

14 See the Retention Obligation (Telecommunications Data) Act.
required for amounts exceeding that limit. And the technology poses another security risk: no technology is ever 100% safe and theoretically cash cards for contactless payments or smartphones with NFC technology can be hacked or skimmed.

Data processing as well as transactions must be carried out safely. The Dutch Data Protection Act states in article 13 that the data controller must take appropriate technological and organisational measures in order to safeguard personal data (see also article 17 of the Privacy Directive). The relevant criteria in this respect are the nature of the personal data, the state of the art and the costs involved in implementing the planned measures.

The Dutch Data Protection Authority published Guidelines in 2013 to give organizations an idea of how to fulfill the security requirements. These Guidelines state that financial data is considered to be sensitive information. The parties involved in contactless payment will have to pay great attention to the security requirements.

The right balance between safety, speed and ease of use needs to be found when drawing up the security requirements. On commencement of a payment transaction, the authentication mechanisms for such payment transactions must include the necessary measures for fulfilling the requirements pertaining to data protection. For example, the number of parties that can access this authentication data must be limited to those parties that are absolutely essential to the carrying out of the payment transaction.

3. Data Breaches

The risk of data breaches follows on from the safety aspect. The Dutch Telecommunications Act already contains – in line with the ePrivacy Directive – a notification requirement for telecom providers with respect to data breaches. Telecom providers must report any infringements of the security measures to the Dutch Authority for Consumers and Markets (ACM) if such breaches will have an adverse effect on the protection of personal data. Reporting data breaches to the data subjects is compulsory if the infringement will probably have an adverse effect on their privacy.

Pursuant to the Dutch Bill on Notification of Data Leaks (Wet Meldplicht Datelekkens), the notification requirement for data breaches will also apply to other data controllers. A new Article 34a to be added to the Dutch Security Obligations

The question whether consumers will embrace contactless payment depends entirely on whether this method of payment is safe. If you lose your contactless cash card or your smartphone with NFC and someone else finds it, theoretically they can use it to debit your account. However, this will always be restricted to the limit you yourself have set for contactless payments. A PIN code is still

d) Consent

If the processing of the personal data cannot be legitimized based upon the execution of a contract, legitimate interests of the data controller or a third party, or if no statutory obligations exist, your personal data relating to contactless payment may only be processed on condition that you have given your unequivocal consent to this. The parties involved will have to ask you to consent for example to the use of your data for marketing purposes, insofar as you are not an existing client. Data controllers may also request your consent for new data processing for which no other grounds were already in existence, such as using or sharing data on your location or income. If sensitive personal data is to be processed as well – such as medical data, if you buy medicines at a pharmacy – your explicit consent will be required.

IV. Other Privacy Obligations

Besides formulating the purposes for processing data and having a basis for this, several other obligations apply pursuant to the Dutch Data Protection Act.

1. Information Duty

Pursuant to article 33 of the Dutch Data Protection Act, the data controller must inform the data subjects on the processing of their data. This article is an implementation of article 10 of the Privacy Directive (see also article 11 of the Draft Data Protection Regulation). The information obligation laid down in the Dutch Data Protection Act entails the requirement to provide information such as the controller's identity, the purposes for which the data is processed. The Draft Data Protection Regulation further specifies and elaborates the information duty in articles 13 and 14. The information provided must always be comprehensible and remain accessible for the data subjects. For example, the data controllers can fulfill their duty to disclose information by posting a Privacy Policy on their website. Moreover, banks can provide the data subjects with this information when they open an account or apply for a new cash card. And telecom providers can send the information to the smartphone of the data subjects as an SMS message, or in the form of operating conditions for an app.

2. Security Obligations

The question whether consumers will embrace contactless payment depends entirely on whether this method of payment is safe. If you lose your contactless cash card or your smartphone with NFC and someone else finds it, theoretically they can use it to debit your account. However, this will always be restricted to the limit you yourself have set for contactless payments. A PIN code is still

---

15 Court of Justice of the European Union, Digital Rights Ireland Ltd (C-253/12) vs. the Minister for Communications, Marine and Natural Resources et al., and Kärntner Landesregierung (C-594/12) et al., 8 April 2014.

16 At an event organized by Hewlett Packard in Tokyo in November 2014 security experts managed to demonstrate ways to break smartphone software and found several bugs in the NFC payment system on many handsets. See: http://www.bbc.com/news/technology-30036137.
Data Protection Authority and to the data subjects. A Bill Y The amended Bill now states that only data The data controllers are obliged to conclude a Data Pro­
cessing Agreement with each data processor (article 14 of the Dutch Data Protection Act). In these agreements, the parties need to agree that the data processor may only process personal data according to the data controllers' instruc­
tions; the data processor may not process the personal data for its own purposes. Moreover, Data Processing Agreements must provide sufficient guarantees relating to technological and organisational security measures with respect to the processing operations. The Guidelines on the security of personal data of the Dutch Data Protection Authority cite a number of points that the Authority takes into consideration when assessing a Data Processing Agreement. These include a description of the services provided by the data processor, the reliability requirements that apply to the processing opera­tions, agreements on the security measures taken, transparency concerning any security incidents that occur and agreements on whether sub-data processors may process data or not.

5. Retention Period
As a general rule, personal data may not be stored for longer than is necessary for the purposes for which it is processed (article 10 of the Dutch Data Protection Act and article 6 (e) of the Privacy Directive). Consequently, the retention period can differ according to each purpose. In such cases, the data minimisation, proportionality and subsidiarity principles are also involved. Normally, consumer data may not be stored for more than 2 years after termination of the contract, in accordance with the Exemption Decree that forms part of the Dutch Data Protection Act. This means that the Dutch Data Protection Act, in line with the Privacy Directive, sets maximum retention periods. In other words, personal data may not be stored for longer than the prescribed term, unless a minimum retention period has been set on the basis of other regulations such as the fulfilment of tax-related obligations.

6. Notification Duty
In principle, each data controller must notify the processing of personal data to the Dutch Data Protection Authority or to an internal Data Protection Official, unless they are able to invoke exemption from the notifi-
cation requirement based on the Exemption Decree (article 27-30 of the Dutch Data Protection Act and article 18 of the Privacy Directive). A number of exemptions may be made in connection with contactless payment, such as exemptions pertaining to the processing of consumer data respectively the processing of communication files. Data controllers will always have to fulfil all the conditions governing the relevant exemptions, and it is advisable to notify the data processing operations if in doubt.

7. Data Transfers Outside the EEA
Additional obligations apply in cases where data controllers transfer your personal data – which includes making this data accessible – to countries outside the European Economic Area (see articles 76-78 of the Dutch Data Protection Act, respectively articles 25 and 26 of the Privacy Directive). The nature of these obligations will depend on the business location(s) of the recipient(s) of such personal data and the purposes of the transfer.

8. Rights of the Data Subjects
Finally, as data subject, you have certain rights such as the right of inspection, the right to object and the right of correction (articles 35-41 of the Dutch Data Protection Act, respectively 12-14 of the Privacy Directive). The data controllers must provide you with the opportunity to access your own personal data in order to check whether it is correct and to make the necessary alterations in the event of incorrect data. You also have the right to delete the data, or have it deleted by a third party. Moreover, if your data is processed on the basis of the data controllers' legitimate interest or that of a third party, you have the right to oppose the processing of your personal data due to personal circumstances.

V. Concluding Remarks
Contactless payment seems to be a development that merely heralds the beginning of many new technological options that will be available to us. However, due to the increasingly stringent privacy regulations and increasing awareness in this respect, it is important that all the parties concerned continue to treat consumers' personal data with the utmost care. After all, we as consumers need to know how our personal data is being used, just as we need a safe environment for payment transactions. Once we have spent our money and relinquished our identity, we are not given the opportunity to do this a second time.

About the Authors

Peter Brown is founder of Peter Brown & Associates PLLC, New York. Mr. Brown maintains an active practice in technology, intellectual property, litigation and technology-related transactions. He has broad experience in alternative dispute resolution as an advocate, arbitrator and mediator. As counsel to technology companies and their customers for many years, he understands the practical business needs of parties to business transactions. He and his team negotiate vigorously but with the goal of successfully completing the transaction with the minimum of unnecessary conflict. When he appears in court, he is able to simplify and explain complex technologies and get to the source of disputes involving advanced technologies.

Sandrine Cullaffroz-Jover is an associate in the IP/IT department of ALTANA law firm, based in Paris. She earned a Bilingual Master’s degree of European Business Law and a Master’s degree of Multimodal IT and e-Business Law. She has a deep knowledge of computer system issues and a solid understanding of the related technical environment. She focuses her practice on IT contract management, privacy law and cyber security strategy.

Prof. Dr. Patrick van Eecke is a lawyer registered with the bar of Brussels, and a partner at DLA Piper (Brussels), focusing on e-commerce, e-government, and data protection issues. He is also professor at the University of Antwerp, teaching European Information Technology and Communications Law.

Gönenç Gürkaynak is the managing partner of ELIG, Attorneys-at-Law. He holds an LL.M. degree from Harvard Law School, and is qualified in Istanbul, New York and England & Wales (currently a non-practising solicitor). Prior to joining ELIG, Attorneys-at-Law as a partner more than nine years ago, Gönenç worked as an attorney at the Istanbul, New York, Brussels and again in Istanbul offices of a global law firm for more than eight years. He holds a teaching position at undergraduate and graduate levels at three different universities in the fields of law and economics, competition law and Anglo-American law.

Kaspar Kala is a lawyer at Borenius in Tallinn, Estonia. He obtained a LL.M. degree (Law and Technology) from Tilburg University (cum laude) in 2014. He is a member of Borenius IP/IT practice group and focuses on IT and data protection as well as industrial property matters.

Vonne I. Laan is a lawyer with Van Doorne in Amsterdam, and a member of the Van Doorne Privacy Team. After she earned her master’s degrees in Information law and Public Law, she joined the IP/IT practice group of Van Doorne. She contributed to the publication of the chapter on smart cities in Handboek voor de Wedhouder (manual for the alderman). Furthermore, she is a member of the Netherlands Privacy Law Association (VPR) and the Netherlands Association for Information Technology and Law (NVvIR). She may be reached at laan@vandoorne.com.

Laura Ligouri is a partner at studio legale Pudolano Cavallo in Rome, which she joined in 2004. She is featured in Who’s Who Legal in the areas of internet and e-commerce law. She has been involved in contractual law for more than 15 years. Her work includes all legal aspects of the Internet and e-commerce, as well as the protection of personal data and consumer rights.

Ave Piik is an attorney at law at Bornenius in Tallinn, Estonia, heading its Intellectual Property and IT practice group and focusing on matters relating to data protection, software development and licensing, electronic communications, e-commerce and media. She is a member of the Estonian Bar Association since 2004. Ave heads the Intellectual Property and IT-law Commission at the Estonian Bar Association and holds the position of a Vice President of the Intellectual Property, Technology, Media and Telecommunications Commission at AIA (the International Association of Young Lawyers).

Kai-Uwe Plath is founding partner of the KNPZ law firm in Hamburg and advises on Commercial Agreements, IT/E-Commerce, Data Protection and on all aspects of IP law in the context of M&A transactions. In the IT sector, he was particularly involved in outsourcing projects. Kai-Uwe Plath has been a member of the Hamburg Bar of lawyers since 2000. Before the foundation of KNPZ, he was a member of the IP/IT practice group at Freshfields Bruckhaus Deringer for over seven years. Kai-Uwe Plath studied law at the University of Hamburg where he earned a Doctor of Law (Doc.iur.) degree in Sports Law. He also received a Master of Law degree in the field of International Transactions and Intellectual Property from Columbia University, New York, where he also worked as a research assistant. He spent further parts of his legal training in London and Los Angeles.

Dr. Andrey Rumyantsev, LL.M., is a deputy editor-in-chief of Svaritelnoe Konstitutsionnoe Obozrenie (Comparative Constitu­tional Review), Russia’s leading journal for comparative legal and interdisciplinary studies in constitutional law. He studied law at the Moscow Lomonosov University and obtained his LL.M. and doctoral degree in law (Dr. jur.) at the University of Regensburg. Website at www.law.net.ru.

Raf Schoefs is a lawyer at DLA Piper (Brussels), focusing on information technology and intellectual property law. Raf assists clients in the drafting and negotiating of complex IT agreements and advises on e-commerce related topics, such as data protection, cookies, cloud computing, electronic signatures and internet intermediary liability. Raf also represents clients in IP infringement proceedings. He has published several articles on the legal implications of new technologies as well as on the liability of intermediaries.

Dr. Elisabeth P.M. Thole is a lawyer with Van Doorne in Amsterdam, and leads the Van Doorne Privacy Team. She is recommended in the international independent guides, such as Chambers, Legal 500 and the "International Who is Who of Internet, E-commerce & Data Protection Lawyers". She holds a Ph.D. on software and copyright law (1991). Elisabeth is a regular speaker, and frequently publishes on IT and privacy-related topics, including a variety of books on privacy (2010), IT contracts (2010), open source (2006), e-commerce (2001) and the Y2K problem (1998). Furthermore, she is an editorial member of “Privacy & Informatie” (privacy and information) and “Tijdschrift voor Internetrechts” (journal of Internet Law). Next to this, Elisabeth is a board member of the IT lawyers Association (VIRA), Vice-President of the UIA Data Protection Commission, and a member of the ITechlaw Association, the Netherlands Privacy Law Association (VPR) and the Netherlands Association for Information Technology and Law (NVvIR). Her email address is: thole@vandoorne.com.

Eva C. de Vries is a lawyer with Van Doorne in Amsterdam and a member of the Van Doorne Privacy Team. She is a co-author of the Dutch chapter of Data protection & privacy – Jurisdictional comparisons (Thomson Reuters 2012) and has contributed to the article Exhaustion and Software Resale Rights, published in this journal (CRi 22/011). Furthermore, she is a member of the Netherlands Privacy Law Association (VPR) and the Netherlands Association for Information Technology and Law (NVvIR). Next to this, she is a member of the governing committee of the center urban district of Amsterdam. She may be reached at vries@vandoorne.com.

Ilay Yilmaz is a senior associate at ELIG, Attorneys-at-Law. She was admitted to the Ankara Bar in 2005 and is currently admitted to the Istanbul Bar. She has represented various multinational and national companies and has an extensive experience in the areas of, including but not limited to, media and Internet law, data protection law, IT and telecoms law, compliance, contracts, commercial law, energy market law, and has written various international and local articles published in English and in Turkish.