I. Notification Duties for Cyber Security

In mid-August 2015, the American retailer Target reached a settlement with payment provider VISA concerning the hack of the credit card details of 40 million Target customers that were leaked in 2013. Around the same time the news was dominated by the hacking of the Canadian adultery website Ashley Madison, also known for its controversial add campaign: “Life is Short, Have an Affair”. Due to this hack the personal data of 37 million Ashley Madison customers were published online. Their names, e-mail addresses, passwords, credit card information and even their sexual preferences ended up on the Internet. The impact of this hack is still to be seen,
but clearly it goes beyond the grief of the spouses involved.¹

With the increased processing of data, data breaches have become a fact-of-life. Processing personal data on a big scale goes hand-in-hand with certain risks. By far the biggest threats are the corruption of personal data, the loss of the data, or data becoming accessible to unauthorised persons; in other words the risks of a data breach.² As the examples show, a data breach can occur by means of an advanced hack, but it can also be caused by the use of outdated software or even a simple human mistake, such as the loss of a USB-stick or a password written on a post-it to serve as a reminder.

Globally the number of data breaches is growing considerably.³ Usually only the most serious cases such as the Target and Ashley Madison hacks make it to the headlines. In the Netherlands there have also been various data breach incidents.⁴ For example, the Diginotar affair in 2011 gained much attention, and the Ashley Madison data breach recalled memories to the security incident at the Dutch extramartial dating website Second Love. This incident was however on a much smaller scale and not caused by a hack, but by a programming error.

In combating the risks of data breaches, a mandatory general data breach notification duty, as part of the Dutch Data Protection Act (Wet bescherming persoonsgegevens), will come into force in the Netherlands on 1 January 2016.⁵ As of next year, data controllers carry the risk of being fined if they do not timely report serious security incidents that will or could lead to a data breach to the Dutch Data Protection Authority (DPA) and the affected individuals.

Such a mandatory breach notification duty is not a new phenomenon. Based upon the e-Privacy Directive, telecommunication providers are already obliged to notify data breaches.⁶ Before the e-Privacy Directive was implemented into the local laws of the EU Member States, experience with such a notification duty had been gained in various Member States, such as Germany, Ireland, Spain and the United Kingdom.⁷ A novelty of the upcoming Dutch general notification duty is that it will be mandatory for virtually all types of data controllers to provide breach notifications, regardless of the sector.

The breach notification duty may even impact foreign organisations. A development that is closely linked to the breach notification duty is the introduction of cyber insurance. This article discusses when, according to Dutch law, data controllers must notify a data breach of personal data. In light of the risks that arise as a result of data breach, this article will also look at the role of cyber insurance.⁸ We shall conclude with an overview of measures to prevent a data breach and/or to minimise its consequences.

II. The Dutch General Data Breach Notification Duty

As of 2016, serious data breaches of personal data will have to be reported without undue delay to the Dutch DPA (Reporting Duty) and the affected individuals (Notification Duty) under the upcoming Dutch law.⁹ Next to that, the enforcement power of the Dutch DPA will considerably increase. Furthermore, the name of the Dutch DPA will change from College Bescherming Persoonsgegevens into Autoriteit Persoonsgegevens (Authority Personal Data).

With the new rules, the Dutch legislator is anticipating the proposed GDPR, which will introduce, among other things, a general notification duty for data breaches that will apply to all data controllers that fall under the scope of the GDPR.¹⁰ The new Dutch rules will apply until the GDPR comes into force, which is currently expected to come into force around 2018. Even though the Dutch general data breach notification duty has only temporarily effect, the Dutch legislator considered it desirable to amend the Dutch Data Protection Act in order to face serious data breaches straight away.

1. On Whom Lies the General Data Breach Notification Duty?

Like any other obligation under the Dutch Data Protection Act, the general data breach notification duty is addressed to the data controller. The data controller is the legal person or public body who determines the purposes and the means of the data processing activities. In that sense, the general data breach notification duty rests on all private and public organisations in the Netherlands who fall under the scope of the Dutch Data Protection Act. Only particular types of organisations, such as

---


² In line with the GDPR, the new article 34a of the Dutch Data Protection Act speaks of a “security breach”. The GDPR defines a “personal data breach” as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” (version of the Council of the European Union of 13 June 2013; http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf).

³ See for example: Privacy Rights Clearinghouse (Chronology of Data Breaches), Gemalto and Safenet (the Breach Level Index) and ‘Worlds Biggest Data Breaches’ visualized on: Information is Beautiful

⁴ See also the EU evaluation report on the tackling of cybercrime of 24 August 2015. In this report, the approach to tackling cybercrime in the Netherlands was evaluated. By means of peer review the implementation and application of the European policy concerning the prevention and combating of cybercrime was examined in each Member State. The Netherlands was evaluated as the second Member State.


⁹ We have introduced this wording, next to the more commonly used term ‘general data breach notification duty’, in order to make it clear that there will actually be two separate duties to notify data breaches.

¹⁰ 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 (General Data Protection Regulation), COM/2012/011 final – 2012/0011 (COD).
telecommunications providers and financial organisations, are exempted from the new general data breach notification duty as sector specific notification obligations apply to these.

2. Cross Border Data Breaches

Although the new Dutch rules are – mainly – related to the Dutch legal sphere, it is to be expected that many data breaches have cross border elements.\(^{11}\) For example, the data controller may be established in the Netherlands, while the breach may occur in another Member State, for example if facilities were hacked there. It may also happen that the Member State where the breach took place, does not coincide with the location of most affected individuals, or that the data breach has happened simultaneously in various establishments (perhaps even in different countries from one another) of the data controller. In all these cases (and possibly others), there may be a need for the local data protection authorities to coordinate.

During the parliamentary negotiations of the Dutch Bill, the international impact of the general data breach notification duty was discussed only briefly.\(^{12}\) Once the GDPR will come into force this may well be less of an issue but until then, multinationals with establishments within the Netherlands or foreign companies that cooperate with Dutch organisations for example, must ascertain whether they might be faced with the Dutch general data breach notification duty.

In accordance with Article 4 of the EU Privacy Directive, the Dutch Data Protection Act applies to the processing of personal data carried out within the context of the activities of an establishment of a data controller in the Netherlands. If the data controller – who may also be established outside of the Netherlands – thus would have an establishment in the Netherlands (which could be a legal entity or a branch office only), and in the context of the activities of such establishment a (potential) data breach occurs, than that data controller should take into account the Dutch general data breach notification duty. A multinational can thus be confronted with the Dutch general data breach notification duty in the event of a data breach occurring in its Dutch establishment. It may also be the case that the Dutch general data breach notification duty is relevant when more than one entity is involved with the processing of the same personal data, for example on the basis of joint or differentiated responsibility. The responsibility may lie with one or more establishments of the data controller within or outside of the Netherlands. In such a case, the establishment outside of the Dutch borders can also be confronted with the Dutch general data breach notification duty and its consequences.

The general data breach notification duty can also be of relevance if the processing activities have been outsourced to a data processor, for example to a payroll service bureau, a call centre or a hosting provider. Such a data processor can be located inside or outside the Netherlands. Regardless the data processors location, data controllers that fall under the scope of the Dutch Data Protection Act are advised to check the service and data processing agreements with their data processor(s) in order to ensure that these agreements take into account the new notification requirements. In turn, data processors should be aware that the new Dutch rules might also apply to them, as they may be held liable for data breaches. In most instances they are the first to be aware of a data breach.

3. Appropriate Security Measures

The breach notification requirement should be considered within the context of the existing security obligations that rest upon data controllers. In line with Article 17 of the EU Privacy Directive, the Dutch Data Protection Act requires that the data controller implements appropriate technical and organisational measures to secure personal data against loss or against any form of unlawful processing. These measures should guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the personal data to be protected. Each situation must be assessed individually in order to identify the appropriate security measures for the case at hand. As in practice it is not always clear what is to be understood under appropriate security, the DPA offers some guidance in its guidelines, which were published in 2013. These guidelines replaced the 2001 guidelines (AV23).\(^{13}\) With the help of the 2013 guidelines, organisations should keep verifying whether their security measures are up-to-date.

4. The Notification: When and to Whom?

Under the new Dutch law, data controllers will be required to immediately report the DPA on any data security breaches that have or are likely to have serious adverse consequences for the protection of personal data (the Threshold Test for the Reporting Duty to the DPA).\(^{14}\) In addition to notifying the DPA, data controllers will also be required to notify affected individuals immediately once there is a reason to believe that the breach could lead to adverse consequences, unless the compromised data is encrypted or otherwise unintelligible to third parties, e.g. by hashing or secure deletion (the Threshold Test for the Notification Duty to the Data Subjects). If the data controller is obliged to inform the data subjects and fails to meet this obligation in time, the DPA might give an order to do so.

5. The Report of a Data Breach to the DPA

The report of a data breach to the DPA as well as the notification to the affected individuals must at least contain information on the nature of the breach, the entities

---

13 See (in Dutch): https://cbpweb.nl/richtsnoeren-beveiliging-van-persoonsgegevens-2013. Other national privacy supervisory authorities, such as in France, Belgium and the United Kingdom, have also published guidelines. See further the 2014 published guidelines by the European Agency for Network and Information Society (ENISA) on security measures for Article 4 and Article 13a, December 2014, https://www.enisa.europa.eu/activities/Resilience-and-CII/Pages/security-measures-for-article-4-and-article-13a.

14 For transparency purposes it would be logic if the Dutch Data Protection Authority, in line with the GDPR, would also choose for a maximum of 72-hour time notification requirement (version of 15 June 2015).
or bodies that can provide further information on the breach, the expected consequences of the breach for the data processing, the recommended measures to mitigate the adverse consequences of the breach, and the measures that can be taken to deal with the breach. When notifying the nature of the breach a general description is in principle sufficient. Recommended measures, which the data subject according to the Dutch legislator can take to mitigate the adverse consequences of the breach, include the alteration of usernames and passwords. The notification to the DPA will also need to contain information of a technical nature, such as a description of the identified and suspected impact of the breach on the processing of personal data and the measures which have been taken or have been recommended in order to mitigate the consequences of the breach. In these cases, data controllers have the right to also explicitly state whether confidential company related information is involved in order to avoid publication thereof.

The data controller will also have to include its contact details in the notification so data subjects know whom to contact if they have any questions. If the data controller has appointed an internal data protection officer, which under current Dutch law is (still) optional, all questions about the incidents could also be directed to this official. Nevertheless, the organisation remains ultimately responsible for the settlement of the consequences of the breach.

6. Internal Data Breach Register

The new Dutch law also compels data controllers to keep an internal overview of all the notifications made to the DPA of data breaches that have occurred. Such overview must at least contain the facts about the nature of the breach and the information that has been sent to the data subjects (if any). On the basis of this reporting obligation data controllers should learn from past data breaches. There is no duty to make the register public, but the DPA may ask for access to the overview and/or demand a copy of the documentation. In view of that, it is conceivable that organisations might choose to have “a double administration”, which is of course not the intention of the Dutch legislator.

When personal data is processed while maintaining the register (for example when monitoring the employees while they carry out their security tasks), data controllers should realize that they should then also take the privacy rules into account. In certain circumstances it may be that consent of the works council is also needed for the processing of the personal data of the employees involved.

7. The Format of the Notification

The Dutch legislator has opted for a form free notification, but further rules can be adopted for the manner in which the notification must be made to the DPA and the data subjects. The DPA shall publish a form on its website for the report to the DPA. In our opinion report to the DPA should ideally be made in secure manner and should be followed by an immediate (automatically generated) confirmation of receipt from the DPA. In this way, the data controller will be able to prove that it has reported the DPA in time.

The data controller shall have to take care that only persons that are authorised to represent the organisation will be allowed to do the notification, and that no information on the data breach will be spread (beforehand) by other means (e.g. by the employees via the social media). Incomplete, false or faulty notifications, which could lead to non-compliance with the general data breach notification duty, are risks carried by the data controller (see further below on the possible sanctions).

Although the new law is silent on this, we believe that multinationals should be able to communicate with the DPA in English, especially as data breaches may not always be limited to the Dutch legal sphere. The same should apply to the duty to maintain the data breach register. This should ensure that all documents are easily accessible in one and the same language.

In order to guarantee an adequate and thorough provision of information when notifying a data breach, the type of breach, the consequences of the breach for the processing of the personal data, the circle of those affected and the expenses involved in the execution, should be taken into account. Each data breach will have to be assessed individually to find the most suitable and appropriate way to notify.

The Dutch legislator speaks of a notification duty to the singular “data subject”. Therefore a duty to notify may exist even in the case of a data breach only affecting one single data subject. Communication means may for example include e-mail, phone, text, social media or in the form of a written letter. If an organisation does not have the contact details of all the data subjects, or if not all of the data subjects are traceable, it may suffice to provide a statement in the form of a suitable medium (for example a newspaper). Whether this is possible will depend again on matters such as the type of breach and the risks involved, the measures which can be taken by the data subjects to reduce any damage, the circle of data subjects, their location, the manner in which normally communication would be sought with the data subjects and the costs involved. A good media- and communication strategy to be decided on at board level is certainly recommended.

Currently the DPA is working on a guidance document, of which a draft version has been distributed for consultation to a limited circle. The DPA has announced that it will come with an adapted, formal version that it will submit for consultation in September 2015. These guidelines should offer the necessary insight on which incidents exactly should be notified and how. To do so, the DPA has indicated that it will take into account the experience previously gained with the (now three-year-old) notification duty for telecommunication and Internet service providers.16

During the negotiations for the Bill, it was estimated that on a yearly basis at least 66,000 notifications are to be expected.17 Judging by the limited enforcement ability of the DPA it is no given fact that the DPA will be able to...
investigate all notifications, let alone take action on all of them. Ultimately, it is up to the DPA to state its priorities when it comes to managing the notified incidents. Data controllers can only hope that it will soon be clear what these priorities are.

III. Insuring Data Breaches

Cyber insurance, which covers data breaches, has been on offer since the 1990's. The cyber insurance originates in the United States where it is known as Cyber Liability Insurance Cover (CLIC). Meanwhile, this kind of insurance is offered by more and more insurers.

When the taking out of cyber insurance becomes an increasing practice, it is likely that organisations will be expected to adjust their insurance portfolio so that (potential) data breaches are covered. This will certainly apply to international operating organisations that process a large amount of sensitive personal data. It is possible that courts and the DPA will take into consideration the insurance aspect when evaluating the liability as a result of data breaches. It is also recommendable to require a service provider, if engaged, to insure himself in line with market practice.

1. Possible Legal Actions in Case of a Data Breach

In the event of a (potential) data breach, a data controller can be faced with various legal actions. The affected data subjects can hold the data controller liable for the consequences of the data breach on the basis of tort. In the Netherlands this involves being held liable for the violation of a legal duty (the security duty). Even though determining (financial) damage can prove to be difficult, the data subjects are able to claim it. A reasonable calculated amount of compensation for the endured immaterial damage can also be claimed. Furthermore, the data subjects are entitled to all their rights under the Dutch Data Protection Act, which include the right of access, the right to correct, and also the right to object to the processing of its personal data. If the data subject has consented to the processing of its data, then that data subject may always withdraw its consent.

If the data breach is caused through actions or negligence of the service provider, then that service provider can also be held liable. The data controller may call the service provider to account, in which case the content of the (mandatory) data processor agreement will be decisive. Both the data controller and the data processor can escape liability if the defence of force majeure is successful.

a) Risk of Enforcement Measures

The DPA can carry out several enforcement measures on request of the data subject, a third party or on its own initiative. The DPA can conduct an investigation into the security measures taken and the correctness of the notification. On top of that, the DPA can ask for additional information, request documents and copy these. Subsequently the DPA has the possibility to take coercive administrative action or impose an incremental penalty. In the case of coercive administrative action the violation will be undone on the violator’s expense while an incremental penalty must be paid until the obligation set by the DPA (such as the recovery of a data breach) has been fulfilled.

b) Sanctions

Under current law the DPA’s power to impose fines is limited. As of 1 January 2016, failure to comply with the main privacy obligations, including the mandatory notification of security breaches, will be punishable with a maximum fine of € 810,000, or in the case of a legal entity, 10 % of net annual turnover from the previous year, if the DPA deems this a more suitable punishment. The fine cannot be imposed until a ‘binding instruction’ has been issued, unless the violation has been committed intentionally or is caused by serious culpable negligence, in which case a ‘tit-for-tat’ policy will apply. As soon as the GDPR will come into force, fines imposed for privacy violations can rise up to € 1 million or 2 % of the company’s worldwide annual revenue (version of the GDPR of 15 June 2015).20

The decisions of DPA are (generally) made public, which can lead to reputational damages.

2. Insufficiency of Traditional Insurances

Cyber insurance covers all kinds of damages and costs caused by and/or associated with a security incident or a data breach. This includes reputational damage, damage as a result of business interruption and loss of profit as well as the forensic and legal costs and the expenses made in order to restore data. As part of the cyber insurance, the insurer may also offer support so that the incident is dealt with in a quick and effective manner and provide help to avoid any future incident.

Within the Dutch insurance market a differentiation can be made between two main types of insurance: the company liability insurance (AVB) and the professional liability insurance (BAV). The AVB covers only property damage and personal injury. Professional misconduct is not included. It is the BAV that covers pure financial loss caused by professional misconduct. A data breach gives rise to pure financial loss. However, this damage is not necessarily caused by professional misconduct. As a result, the damage caused by the data breach cannot be covered by the BAV. But it cannot be covered by the AVB either as there is no property damage or personal injury.

Besides the damage suffered by the data subjects, a data breach often involves damage to the organisation. Such damage is also not covered by the AVB or BAV and is difficult to quantify. It is difficult for example to estimate the extent to which the organisation’s reputation has been damaged.

Even the insurance against damage to business – which insures the risk of business interruption caused for example by fire or lightning – is not adjusted to the new cyber risks. An organisation that has suffered a data breach caused by a virus or a hack will therefore not be compensated under the existing insurance.


19 The new law refers to the sixth category of Article 23 sub 4 of the Dutch Penal Code, which currently is equal to the maximum amount of € 810,000, but this may increase after 1 January 2016.

3. First & Third Party Damage
Generally a distinction can be made between first and third party damage. First party damage consists of costs made by the organisation itself in case of an incident. If this involves a data breach, one can think of the costs made to restore the data and the system. Third party damage relates to the costs involved with being held liable by a third party. Here one can think of legal costs and expenses and the compensation that must be paid to the data subjects.

4. The Scope of Coverage
When taking out cyber insurance, organisations must keep close track of the conditions that they must satisfy in order to be able to cover their damages and costs. They must also check which damages might be covered by another insurance or require additional insurance.

A difficulty for insurers is that the damage related to a data breach is often unclear and undefined. Data that is being processed is not physical but in the form of digital matter and is often not found in one place only. Many IT-systems are interdependent. This can give rise to questions concerning responsibility and insurance of the damage. In order to get a good idea of the risks involved, companies should keep the insurers up to date about their privacy and security policy. Insurers should consult IT-experts who are well informed on matters such as computer security, process and risk management.

5. Insurance Cover of Fines
Traditionally insurance policies do not cover fines in relation to data breaches. There are however cyber insurances that do offer such coverage. This is a tricky issue in itself: insuring fines takes away their incentive and this can be seen as a violation of public policy. This is especially the case with fines imposed as a result of intentional behaviour. An organisation does not act with intent if it has taken all necessary security measures, but it is nevertheless hacked. There are insurance companies that deem insuring a fine under those circumstances acceptable.

IV. A Data Breach Response Plan
Even with cyber insurance, organisations must do prevent a data breach and/or minimise the consequences as much as possible. An integrated and multi-disciplined approach from privacy and IT-perspective, as well as an adequate media and communication strategy by means of a data breach response plan is highly recommended. The measures can be divided into three stages: the phase before the data breach occurs (preventative measures), the phase during the data breach and the phase after the data breach has taken place (repressive measures).

1. Preventative Measures
In order to avoid a data breach, it is important that during the first stage as many preventative measures are taken as possible. More and more parties are providing assistance such as Hacking-as-a-Service (HaaS), whereby the security system of an organisation is inspected periodically on the basis of a subscription so that vulnerabilities are found and remedied. Some organisations have opted for a Responsible Disclosure Policy on their website. The aim of this policy is to invite ethical hackers – often in exchange for a financial reward – to expose the weak spots in the data processing.

A privacy impact assessment (PIA) must be carried out before personal data can be processed. This assessment should provide insight into risks that go hand in hand with the processing of data and privacy requirements that must be met. An organisation will have to keep in mind the type and amount of personal data that is being processed while carrying out a PIA.

2. Repressive Measures
Experience has shown that the first 24 hours after an incident has taken place are the most crucial when it comes to damage control. This means that at that moment, measures to recover the data and minimise the damage should be taken straight away. It must be assessed urgently whether the data breach has to be notified to the data protection authority. Furthermore, it must be decided which statement is to be made public. It is advisable to have a stand-by team dealing with incidents ready at all times.

After a data breach has occurred, recovery measures must be taken which involve for example, the reduction of personal data – so that the data breach will not infect other data – and backing up the system on which the data is saved. The team dealing with incidents shall have to investigate the data breach and must scrutinise how future data breaches can be avoided. It is recommended to document all taken steps.

V. Concluding Remarks
Data subjects should expect organisations to process their personal data diligently, especially if these are data of a sensitive nature. Time will tell if the (temporary) Dutch general notification duty really will lead to an increase in the protection of privacy for the data subjects until the GDPR comes into force. In any case, data controllers – which may also be located outside the Netherlands – will have to take the necessary protective and reactive steps as part of their risk minimisation strategy. In this regard it is advisable to also look at the insurance portfolio. The more common cyber insurance becomes, the more it is likely that it will be taken into account by both the courts and the DPA when assessing claims as a result of data breaches. For all stakeholders these are all interesting developments, which they will not be able to ignore in the coming years, and so there is actually only one real recommendation that counts: “Life is Short, Avoid a Data Breach Affair”.

---

within the corporate commercial department at ENSafrica. She specialises in technology, broadcasting and telecommunications law as well as data privacy and protection.

**Sapna Mehta** is associate of Fenwick West LLP in Mountain View, California. She focuses her practice on a broad variety of litigation matters to support clients in the high technology and life sciences industries.

**Anneke Meiring** is a senior associate in the corporate commercial department in ENSafrica’s technology, media and telecommunications (TMT) team. She specialises in digital entertainment and technology. She has extensive experience and expertise in the TMT sector, which she gained at local and international mobile network operators, a UK based quad player, a local internet service provider and public broadcaster.

**C.R.M. (Carl) Moll** is a LLM Dutch Commercial Civil Law student at Universiteit Utrecht. As part of the university’s honours programme he attended Utrecht Law College, where he completed his bachelor’s degree in Dutch Law. Carl spent one year at the Université Panthéon-Assas in Paris where he studied French Commercial Civil Law. As well as completing his degree, he is currently working in a renowned Dutch law firm as a legal assistant and is active in multiple study associations.

**Tyler Newby** is partner at Fenwick West LLP in San Francisco, California. He focuses his practice on privacy and data security litigation, counseling and investigations, as well as intellectual property and commercial disputes affecting high technology and data driven companies. Tyler regularly advises companies large and small on responding to data security incidents, and has an active practice in defending companies in consumer class actions, state attorney general investigations and federal regulatory agency investigations arising out of privacy and data security incidents.

**Yajas Setlur** is a Junior Associate in the Technology Practice Group of J. Sagar Associates and is based in Bangalore, India. He assists in advising clients on data privacy issues and information technology laws in India. He may be contacted via phone (+91–99 1 8 9 2 528) or email (yajas.setlur@jslalaw.com).

**M.C.S. (Charlotte) Gräfin zu Solms-Sonnenwalde** completed her bachelor’s degree in Dutch Law at the Universiteit Utrecht’s honours programme (Utrecht Law College). During her degree she was active in various law related study associations. In line with her international background, Charlotte is now continuing her studies at the University of Edinburgh as a master’s student in the field of International Law.

**Dr. Elisabeth P.M. Thole** is a lawyer with Van Doorne in Amsterdam, The Netherlands. She leads the Van Doorne Privacy Team and is also a member of the Van Doorne Cyber Response Team. Elisabeth is recommended in the international independent guides, such as Chambers Europe (Band 1), Legal 500 EMEA (Tier 1) 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 & Information” (privacy and information) and “Tijdschrift voor Internetrecht” (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: tboile@vandoorne.com.

**Lauranne Truyens** is an associate at the Brussels law firm Altius, where she focuses on ICT, commercial law and privacy. She already assisted hardware manufacturers, software developers, system integrators, e-commerce players, telecommunications operators and suppliers of other ICT-related services. She regularly advises on data protection, e-commerce, digital signatures, trade practices matters, including (on-line) advertising, and general commercial law. Lauranne graduated from the University of Antwerp, and obtained an LLM degree in Information Technology, Media and Communications law from the London School of Economics and Political Sciences.

**Gerrit Vandendriessche** is a Partner at the Brussels law firm ALTIUS where he runs the ICT practice. He has a general commercial background with a strong focus on ICT-related matters. He assists hardware manufacturers, software developers, system integrators, e-commerce players, telecommunications operators and suppliers of other ICT-related services such as consulting, support and maintenance services. He regularly advises on data protection, e-commerce, digital signatures, trade practices matters, including (on-line) advertising, and general commercial law. He also conducts ICT-related litigation.

Gerrit Vandendriessche graduated from the University of Leuven, Belgium (Lic. Jur., 1996) and obtained a special degree in Information Technologies and Communication Law in 1997 from the University of Namur, Belgium. Gerrit has been a member of the Brussels Bar since 1997. Gerrit Vandendriessche is also a freelance researcher and guest lecturer at the Free University of Brussels (VUB). He is the author of an ICT law book and has published several articles on data protection and Internet search engines.