Photo byMichael Traitov on Shutterstock

LEXOLOGY
Getting The Deal Through

Market Intelligence

PRIVACY & CYBERSECURITY 2023

Global interview panel led by WilmerHale

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this *Privacy & Cybersecurity* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Post-covid trends
Cloud hosting
M&A risks
Selecting counsel

START READING

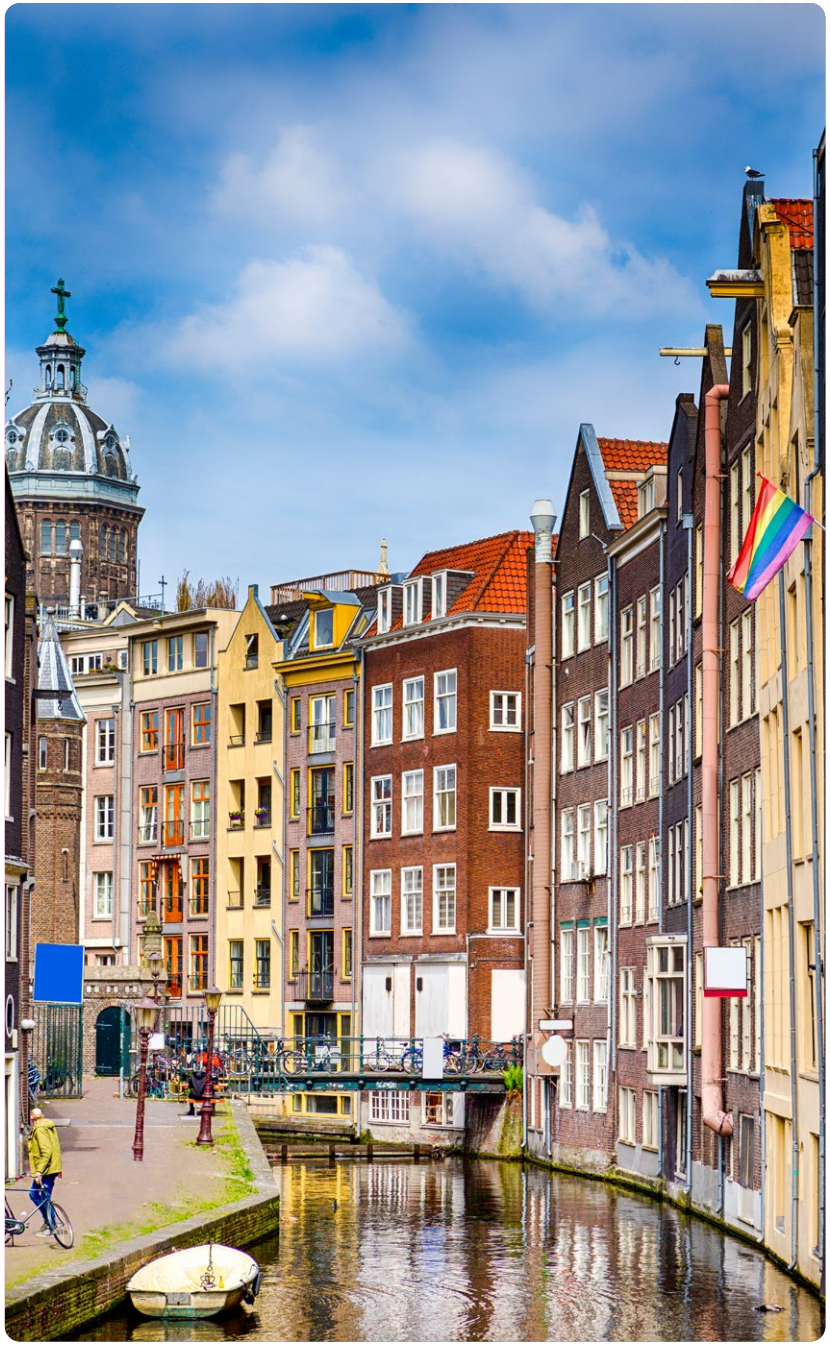


Photo by Dmitry Morgan on Shutterstock

Netherlands

Quinten Kroes heads Brinkhof's data protection practice and has been active as a lawyer in the telecommunications, media and technology (TMT) sectors since 1995, advising on and litigating matters of telecommunications, media and data protection law. He advises a broad range of companies on data protection. He has supported various companies that have been the subject of investigations by the Dutch Data Protection Authority.

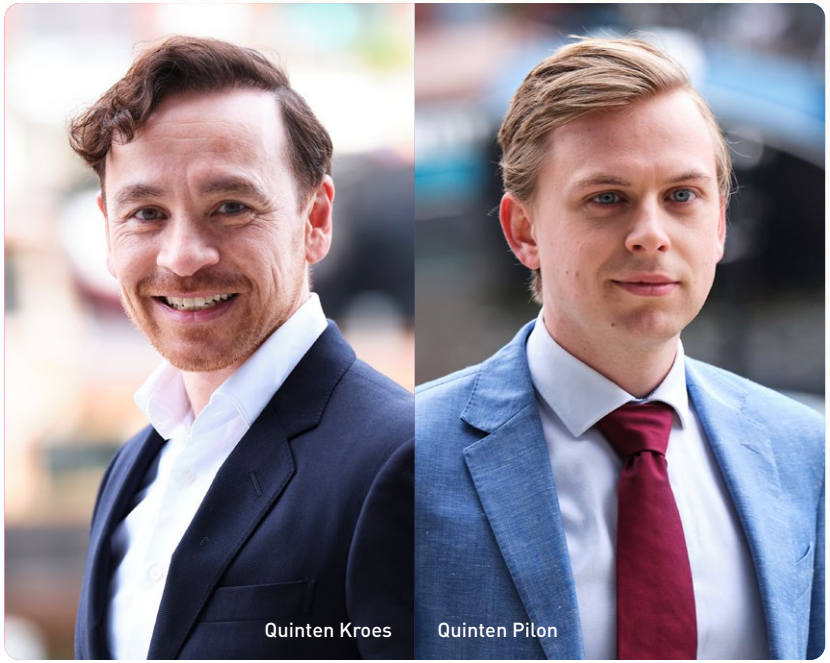
Quinten's reputation is recognised as top tier in legal directories, as is the quality of Brinkhof's data protection practice.

Quinten Pilon is an associate at Brinkhof and specialises in data protection, TMT and competition. He advises clients on a broad range of data protection and cybersecurity-related issues.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

In terms of new legislation, several amendments in the field of cybersecurity are noteworthy. At the national level, an amendment to the Dutch Network and Information Systems Security Act law entered into force on 1 December 2022, which allows the National Cyber Security Centre (NCSC) to share information about cyber threats with the private sector. Previously, the NCSC was only allowed to inform and advise vital providers and government bodies with up-to-date threat and incident information about their network and information systems. Under the new system, 'linchpin organisations' can receive threat and incident information from the NCSC. These linchpin organisations can in turn share that information with their constituencies. An example of such a linchpin organisation is the Digital Trust Centre, part of the Ministry of Economic Affairs and Climate. Other linchpin organisations serve specific constituencies, such as the healthcare or high-tech sectors. Additionally, the NCSC can now also share threat or incident information directly with non-vital providers. This is allowed if there is no linchpin organisation that can provide the non-vital provider with the information and the information concerns a threat or incident with potentially significant consequences for the continuity of the provider's services.

On 18 April 2023, the Dutch legislator also approved the proposal for the (Dutch) Act on Electronic Data Interchange in Healthcare (Wegiz). The Wegiz stipulates that healthcare providers may be required to exchange certain data in electronic form. While the Wegiz regulates how data should be exchanged, it does not regulate whether the healthcare provider is allowed to exchange the data nor the types of data that can be exchanged. What data is exchanged between healthcare providers is determined by the healthcare providers themselves. The Wegiz is expected to enter into force on 1 July 2023.



At the European level, the NIS2 Directive entered into force on 16 January 2023. The NIS2 Directive has widened the scope of the first NIS Directive, introducing a size-cap rule covering medium and large-sized entities from a large variety of sectors. The Directive also applies to some critical and essential entities regardless of their size. Key material changes include detailed rules for incident-reporting, stricter enforcement requirements, the harmonisation of sanction regimes across member states and improvement of cooperation between member states. There is now a two-year period during which all member states must implement the NIS2 Directive's measures into their national legislation.

The Digital Operational Resilience Act (DORA) also entered into force on 16 January 2023 at the EU-level. This regulation creates a firm regulatory framework for digital operational resilience in the financial sectors, by introducing rules for the protection against, and

> "The Dutch DPA will not shy away from using its GDPR powers to go after the violation of other fundamental rights, such as the right to equal treatment."

the detection, containment and recovery of ICT-related incidents. Importantly, DORA does not merely apply to financial institutions, but also to 'ICT third-party service providers'. These are non-financial service providers that provide third-party ICT services to financial institutions. DORA constitutes a lex specialis in relation to the NIS2 Directive. Companies will have a two-year period to prepare for DORA, as its provisions will apply from 17 January 2025.

Aside from these new laws, the main regulatory development has been that the enforcement of the GDPR, by both the Dutch regulator and through collective class action claims, is steadily increasing. So far, the Dutch data protection authority (DPA)'s preferred method of enforcement seems to be the imposition of administrative fines. Cases where it has decided to impose an order or a ban on the processing of personal data, or issued a formal warning or reprimand, are the exception. So far, the Dutch DPA has published 22 fines that it imposed on both companies and government institutions for violating the GDPR. Three of these fines were imposed for a failure to notify a data breach in a timely manner and six fines for failing to implement sufficient security measures. With regard to collective class action claims it is noteworthy that the Court of Justice of the European Union recently ruled that mere infringement of the GDPR does not give rise to a right to compensation. However, the court also affirmed that the right to compensation is not limited to non-material damage that reaches a certain threshold of seriousness. Member states with minimum thresholds for non-material damages, such as the Netherlands, will therefore likely have to accept separate liability regimes for such damages under the GDPR.

Generally, the fines published by the Dutch DPA have been relatively high compared to fines imposed on average in other member states, although not near the level of the highest. The Dutch DPA imposed two record fines of €3.7 million and €2.75 million on the Dutch Tax Administration for illegally processing personal data in its fraud identification facility and for discriminatory and unlawful data processing respectively. Although both cases were quite unique and have also triggered a broader political and societal debate on racial profiling and discrimination, it shows that the Dutch DPA will not shy away from using its GDPR powers to go after the violation of other fundamental rights, such as the right to equal treatment. In concrete terms, it will take violations of other fundamental rights into account in determining the fine for the violation under the GDPR. The Dutch DPA has also imposed fines on relatively small organisations, which are significantly lower than what its fining guidelines suggest. For example, an orthodontic practice was fined €12,000 for insufficiently securing the personal data that patients were uploading to its website. Similarly, lower fines were imposed on a small foundation aligned to a Dutch political party, and an outdoor advertising company that had failed to adequately protect certain HR records.

Several fines that the Dutch DPA imposed have now been challenged in court. In one case, the district court in Utrecht ruled that the Dutch DPA had wrongly rejected the 'legitimate interest' as basis for

the processing of personal data by a company that offered amateur football clubs a platform to film and stream matches. In doing so, the court rejected the Dutch DPA's official position that purely commercial interests can never qualify as a 'legitimate interest'. Moreover, in appeal the Council of State ruled that the platform for amateur football did not have a purely commercial interest, but also a social interest. In another case with a similar question of law, the Amsterdam District Court has referred preliminary questions to the European Court of Justice. In this case, a tennis association had provided personal data to a third party for a fee, without seeking the consent of its members. The referring court has asked whether a purely commercial interest and the interest as at issue here, the provision of personal data for payment without the consent of the data subject, can be regarded as legitimate interests, and if so under which circumstances. Finally, the district court in The Hague found that a fine on a local hospital for its failure to implement adequate access restrictions to patient records was justified, but that the amount of €460,000 was unreasonably high. The court lowered it by €110,000, mainly because the hospital had taken a number of measures to prevent further violations.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

Pursuant to article 33 of the GDPR, a controller must notify a personal data breach to the Dutch DPA, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also, without undue delay, inform the data subjects, communicating in clear and

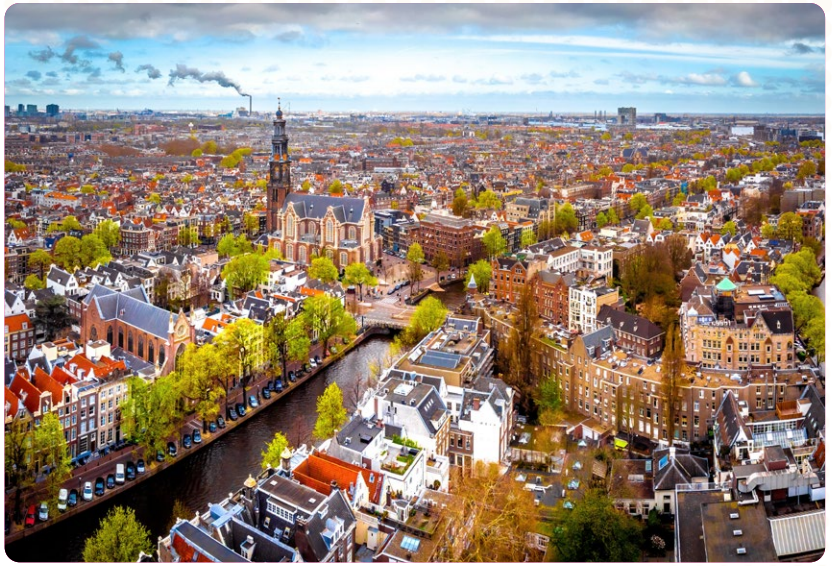


Photo by Alexey Fedorenko on Shutterstock

plain language the nature of the personal data breach (article 34 GDPR). This communication is not required when the controller has taken measures to ensure that the risk of a breach is not likely to materialise. Breach notification requirements similar to those contained in the GDPR already existed in Dutch law since 2016.

The European Data Protection Board's (EDPB) has published guidelines 9/2022 with general guidance on personal data breach notification under GDPR, as well as a separate set of guidelines (01/2021 on Examples regarding Personal Data Breach Notification) with concrete examples of the types of incidents that should be notified. The Dutch DPA also publishes informal guidance on this topic on its website, including its own list of concrete examples.

All these documents make it clear that a number of criteria will be relevant to assess whether a notification needs to be made. These include the sensitivity of the data, the number of data subjects affected, the volume of data lost and the possible consequences for data subjects. Moreover, it is also considered relevant to take into

"The Dutch DPA has stated that paying a ransom to (supposedly) prevent criminals from further spreading personal data after a ransomware attack, does not exempt organisations from notifying the personal data breach to Dutch DPA or data subjects."

account who received the information and to which categories of data subjects the data relate (eg, data relating to children or other vulnerable groups).

The Dutch DPA has also given further guidance on its website specifically on whether ransomware can qualify as a breach that needs to be notified. In short, it takes the position that this is indeed the case, as the illegal encryption of data implies illegal access to data and a circumvention of security measures that should have prevented this. The guidance issued in 2021 by the EDPB confirms this approach. The Dutch DPA also considers that it will often be hard to establish the precise effects of ransomware and to exclude the risk that it may have transferred or manipulated personal data in addition to encrypting the data. The Dutch DPA has stated that paying a ransom to (supposedly) prevent criminals from further spreading personal data after a ransomware attack, does not exempt organisations from notifying the personal data breach to Dutch DPA or data subjects. It does not consider paying ransom an appropriate measure that will prevent high risks to the rights and freedoms of data subjects to materialise. After all, paying a ransom does not guarantee that hackers will actually delete (and not resell) all personal data.

In the case of doubt, the Dutch DPA recommends to submit a preliminary notification of a possible breach. The notification can always be amended or even withdrawn at a later time, when the controller has more knowledge of the breach and its consequences. Controllers can notify through a web-based notification tool on the Dutch DPA's website, which was updated in 2021. Currently, this tool is only available in Dutch. However, an English language questionnaire, which includes all questions of the online notification tool as well as some explanatory comments, is available on the website of the Dutch DPA.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

Companies must continuously assess both the technical and the organisational measures they are taking to protect and secure their personal data. If a security incident occurs the company should give priority to fixing the particular security issue and do its utmost to mitigate the negative consequences of the breach.

Measures to be taken will vary depending on the type of incident, from trying to locate a lost data carrier, to contacting the recipients of an email that was wrongly sent or addressed, remote wiping of a portable device or working with a processor to establish the extent of a security incident in their domain. A recent court ruling confirms that processors may even be ordered by a court to provide detailed information on security incidents if they fail to do so in response to legitimate customer queries. If a hacker may have obtained personal data, the company will have to assess whether or not the data had been sufficiently encrypted, as this is relevant to the question whether a notification should be made. If passwords have been leaked, the company should force users to change these passwords.

A data breach could be an indication that existing organisational and technical measures are not adequate. Maintaining appropriate and adequate levels of security requires continuous efforts and constant scrutiny through risk assessments, planning, executing, checking and doing the same all over again (the 'plan-do-check-act' cycle (PDCA)). The guidance adopted by the EDBP in 2020 on privacy-by-design and privacy-by-default confirms this. This is a logical consequence of the notion that the adequacy of measures must be viewed in light of current technical standards. It does not necessarily mean that technical measures need to be renewed at least annually to match the most advanced security system available. However, at least a suitable

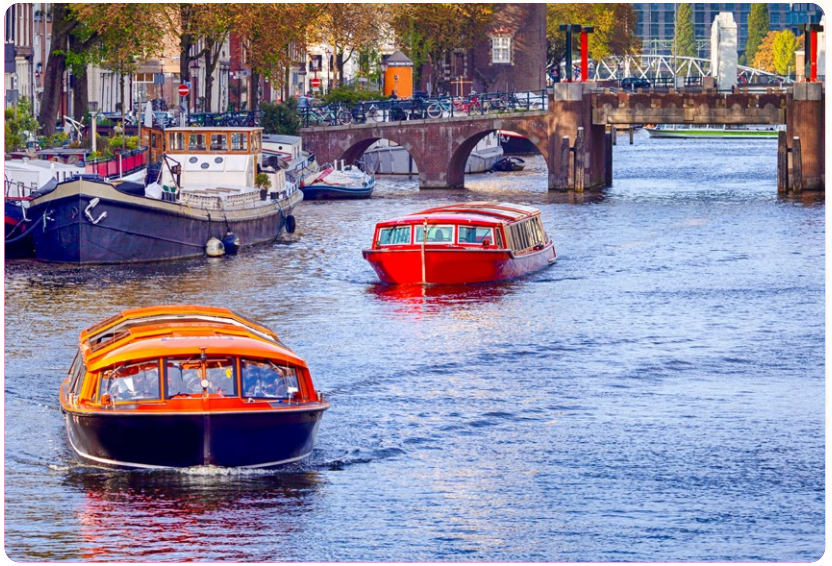


Photo by Dmitry Morgan on Shutterstock

level of proactive monitoring is required: when imposing a fine on the Dutch Employee Insurance Agency (UWV) in July 2021, the Dutch DPA took into account the fact that the UWV did not sufficiently monitor and evaluate its security measures.

The strength of the measures should also be viewed in proportion to the nature of the data it protects. A pizza shop with a spreadsheet of local customer addresses for mailing promotional flyers will not need military-level encryption. But processing of sensitive data will require measures like two-factor authentication, encryption, hashing (both using state-of-the-art algorithms) and/or, if possible, anonymisation or pseudonymisation.

The Dutch DPA considers two-factor authentication to be a common and fairly easy security measure to implement. Increasingly, organisations turn two-factor authentication on by default. According to the Dutch DPA, two-factor authentication is a minimum requirement for securing access to health data. Moreover, it should be borne in mind that the Dutch DPA not only considers the special

categories of personal data as defined in the GDPR sensitive. In the past, it has also recognised other categories of data, such as location data and data concerning someone's media consumption, as sensitive in nature. Failure to comply can have consequences. The DPA has imposed a fine on an airline company for not implementing strong passwords and two-factor authentication in its back office systems, which contributed to a data breach.

Organisational measures to be applied include confidentiality agreements with employees, disabling access to personal data for employees who have no need to use the data, adequate contracts with data processors and the deletion of records at the end of their retention period. Access to data should be logged and the resulting logs reviewed regularly. Adequate measures should also include clear documentation and instructions on what actions to take if an incident occurs. Timing is important; as the Dutch DPA's fine of Booking.com in 2021 shows, professional parties are expected to meet the timelines set out in the GDPR. If the cause and consequences of an incident are not yet clear, companies are advised to file a preliminary notification with the Dutch DPA, and to err on the side of caution.

A recent fine by the Dutch DPA for a local bank furthermore shows that proactive action after a data security incident can significantly reduce a fine following a security incident. The bank was fined due to a data breach caused by poor identity verification by the telephone helpdesk. However, shortly after the incident the bank compensated the affected data subjects and submitted a comprehensive risk inventory and action plan to the Dutch DPA. Subsequently, the bank at its own initiative swiftly implemented a large number of improvement measures relating to their recording practices, system support, testing and assurance, and to increase their internal professionalism and awareness in this field. The Dutch DPA also noted that despite the breach of article 32 GDPR, the bank had taken some prior measures

"A recent fine by the Dutch DPA for a local bank furthermore shows that proactive action after a data security incident can significantly reduce a fine following a security incident."

to minimalise the privacy risks for data subjects. This prompted the Dutch DPA to reduce its fine from €310,000 to €150,000.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

As with any other modern networked society, the Netherlands is very much dependent on digital infrastructure. Statistics by the NCSC show that the vast majority of cyberattacks concern phishing, ransomware and denial-of-service attacks, all of which require vastly different remedies. As a direct consequence of this diversity, the NCSC advises a varied approach. However, as a general observation it can be noted that research shows that it is essential to increase individuals' security awareness, which will not only benefit their security practices at home but also the security of the companies they work for. Updated software and regular backups (patch management) and the need for strong passwords are also essential to resilience against cyberattacks. Using professionally secured cloud services is among the general advice given to companies to increase their security. Large companies are, of course, better equipped to meet the cybersecurity challenges and may also rely on external experts to become more resilient against cyberattacks. The EDPB, however, has recently published a data protection guide specifically for small business, which gives clear and step-by-step instructions for achieving GDPR-level data protection, including practical tips for improving security standards. In general, the NCSC advises companies to divide user accounts into low-, medium- and high-impact accounts, depending on the sensitivity of the data that the account contains and the resources that the account has access to. The report advises to implement more stricter security measures for medium- and high-impact accounts. With regard to ransomware attacks, the NCSC has published guidance entitled Ransomware

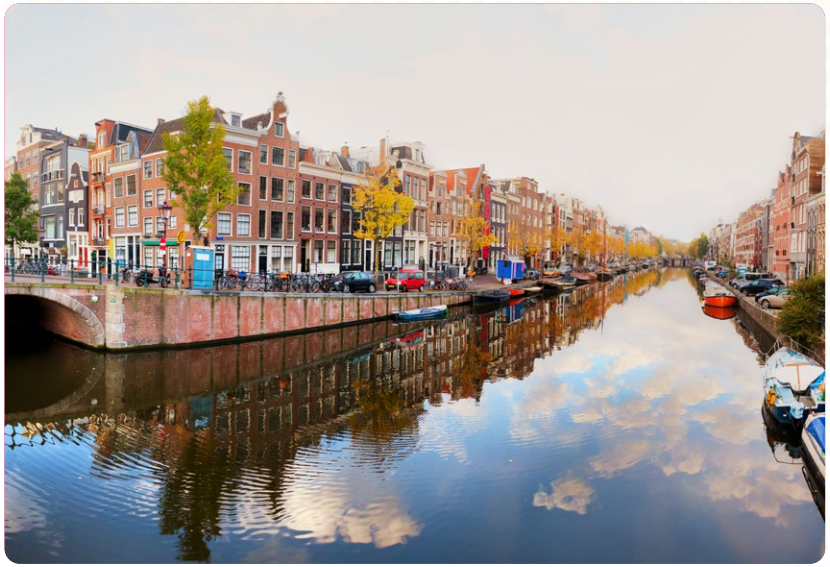


Photo by photo.ua on Shutterstock

Incident Response Plan. This explains how organisations can contain a breach, fix a vulnerability, remove the malware and prevent unauthorised access in the future by following the incident response cycle (Preparation-Identification-Containment-Eradication-Recovery-Lessons learned). Moreover, the NCSC has recommended that organisations scale up network capacity to be able to serve the large number of homeworkers, which has become more normal since the covid pandemic, and imposing appropriate security safeguards. These include forcing the use of a secure connection to the corporate network through, for example, a virtual private network (VPN), making maximum use of multi-factor authentication and enforcing strong passwords. Furthermore, the Dutch DPA has also provided useful guidance to workers on how to work securely from home. It has advised them to only work from a secure work environment, to protect sensitive documents, to use (video)chat services cautiously and to be on the alert for phishing mails.

QUESTIONS

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The controller is, and will, remain responsible and liable for any personal data he or she collects or processes. An important aspect of cloud services is the location where personal data is actually stored and processed. Under the GDPR, personal data may only be processed outside the European Union (or more precisely: the European Economic Area (EEA)) if the third-country where the data is processed provides an adequate level of protection. Compliance can be achieved in various ways, all having to do with ensuring that adequate safeguards are in place within either the company or the country to which the data is transferred.

"The controller is, and will, remain responsible and liable for any personal data he or she collects or processes. An important aspect of cloud services is the location where personal data is actually stored and processed."

However, the EU Court of Justice's ruling invalidating the European Commission's EU-US Privacy Shield approval in the case of *Schrems II* has shown that safeguards in the context of international data transfers can be fragile. *Schrems II* has had far-reaching consequences beyond the Privacy Shield alone, as it also forced data exporters to conduct so-called transfer impact assessments (or TIAs) for data transfers based on standard contractual clause (SCCs) s, and to assess whether 'additional measures' are necessary to guarantee an adequate level of protection. In doing so, this judgment has called into question the legitimacy of international data transfers to not only the US but also to other destinations outside the EEA. The Recommendations of the EDPB that followed it unfortunately do not offer easy solutions for all transfer scenarios either.

Currently, the main way to transfer personal data to the US on a regular basis is by concluding SCCs combined with implementing (individual) transfer impact assessments. The recently adopted SCCs by the European Commission – which had to be implemented by 27

December 2022 – go some way to address the concerns raised by *Schrems II* and contain updated clauses that are aligned with the GDPR. Yet these SCCs can only be relied on by organisations that transfer personal data to non-EEA parties that are not subject to the GDPR. As the larger US-based cloud providers will likely fall under the territorial scope of the GDPR, organisations will, strictly speaking, not be able to rely on the updated SCCs as a transfer mechanism to these cloud providers. The European Commission has, in the meantime, clarified that it is in the process of creating new SCCs for transfers to non-EEA parties that are subject to the GDPR.

Possibly, this uncertain situation will be redressed by the adoption of the new EU-US Data Privacy Framework (DPF). President Joe Biden signed an Executive Order on 7 October 2022 outlining what steps the United States will take to implement the commitments as set out in agreement in principle on the new DPF. The Executive Order includes safeguards to the processing of personal data by US intelligence authorities by limiting the access to data to what is necessary and proportionate to protect national security and the establishment of an independent and impartial redress mechanism. However, the Executive Order faced criticism, including from the European Parliament. This has taken the position that the Executive Order is not sufficiently in line with the *Schrems II* criteria, causing the DPF to be vulnerable to a new legal challenge. It is currently unclear when the DPF will be implemented. Transfers to the UK remain lawful without the need to implement any transfer mechanism, due to the adequacy decision the Commission adopted on 28 June 2021. However, this too could be reconsidered if the UK were to implement changes to its data protection framework.

These developments raise the question whether data localisation is in fact the only robust and long-term solution likely to withstand future legal challenges. With respect to cloud services in general, the Dutch DPA has published a number of guideline that are in line with

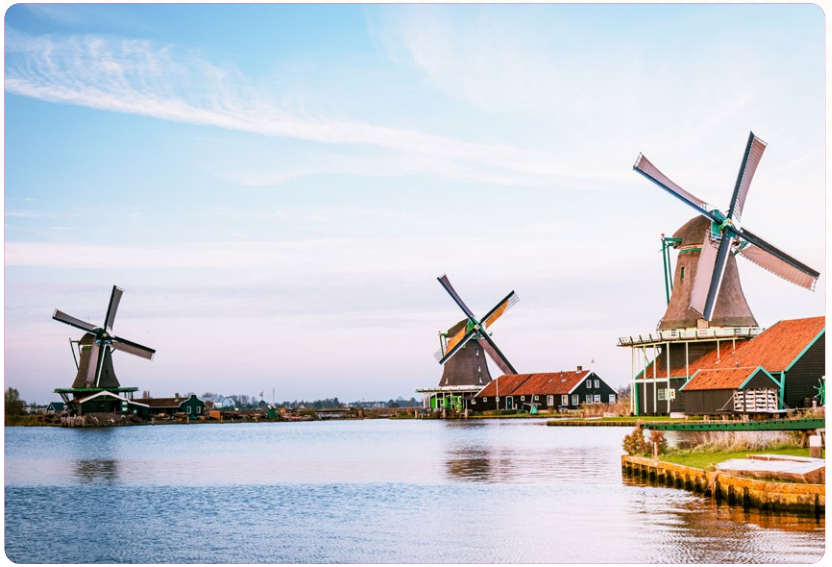


Photo by fokke baarssen on Shutterstock

the former article 29 Working Party's guidance on the issue and that do not raise fundamental obstacles to the nature of cloud computing. For example, the Dutch DPA has taken the view that, even for medical data, there is no need to ask consumers for specific permission for the use of cloud hosted services. But there are also looming signs of a more restrictive view. In January 2022, the DPA published a disclaimer on its manual for privacy-friendly settings of Google Analytics, stating that it is considering a complaint on this cloud-based website analytics tool, which may lead it to conclude that Google Analytics may no longer be used lawfully in the Netherlands. Since then, however, the Dutch DPA has not provided any further comment on this matter.

While this indicates a general openness to cloud solutions for now, using cloud hosting will need to be part of the overall risk assessment the controller makes before moving to the cloud, and one that may need to involve a data protection impact assessment under the GDPR. The Dutch government has itself commissioned various DPIAs into governmental use of commercial cloud services. Interestingly, these DPIAs focus heavily on the processing of diagnostic data by service

providers (ie, data about the use of their cloud services, rather than the data provided by customers). The final reports, which are all available online in English, have guided the government's negotiations with a number of large international cloud providers, and have, for example, prompted Microsoft to amend its privacy policy worldwide. Last year, the Dutch government signed an agreement with Google Cloud that also includes enhanced privacy measures. As a result Dutch government agencies can continue to use Google Workspace in compliance with the GDPR.

"Risk assessment does not stop once the choice has been made for a particular cloud solution: if the cloud host faces security issues, the controller will need to rethink using this particular company."

Risk assessment does not stop once the choice has been made for a particular cloud solution: if the cloud host faces security issues, the controller will need to rethink using this particular company. A first indication of the quality of the host may be found in the availability of certificates (ISO, ISAE, NEN) concerning security. According to article 28 GPDR, adherence to an approved code of conduct may also be used to demonstrate sufficient guarantees. In 2020, the Dutch DPA approved the code of conduct submitted by NL Digital, an association of IT companies, including cloud providers. Similar codes of conduct have been approved at the EU level, most notably the CISPE Code of Conduct and the EU Cloud Code of Conduct.

To assist controllers and processors to determine what 'appropriate technical and organisational measures' (article 34 GDPR) are, the European Union Agency for Network and Information Security (ENISA) has published guidelines that with examples of such measures. ENISA has emphasised that the guidelines do not have a 'legal status', and mainly serve as guidance for market parties. The NCSC shared its own experiences in moving to the cloud, which is intended to help other organisations. In addition, the NCSC published a factsheet containing five general tips for procuring secure cloud-hosting services.

Contractually, it is advisable to address any specific concerns a controller may have in the processor agreement proposed by the

cloud provider. The controller should ensure that the contract allows for access to the data at all times, even in a situation of conflict with the processor. The processor agreement should also address the issue of data location explicitly, as this is a specific requirement under the GDPR and one that may be particularly challenging to address in a cloud-based setting. Other topics that warrant careful deliberation are the provider's duty to support the notification duty of the data controller if a breach should occur in the cloud provider's domain, the provider's transparency on issues like law enforcement cooperation and also the provider's role in processing metadata about the use of its services.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The NCSC was established in 2012. This public–private body advises companies and the government on the usage of software and measures to increase cybersecurity. Its aim is to make the Netherlands more resilient against cybercrime.

In its Cybersecurity Assessment Netherlands (CSAN) 2022, the NSCS concluded that digital risks to Dutch national security remain high. The gravest threats are posed mainly by state actors, cybercriminals and outages. While the Netherlands has taken steps towards more resilience against cybercrime in the past year, the 2022 CSAN reiterates that the current level of resilience is still insufficient. According to the report there is a growing gap between the extent of the threats and the level of digital dependence as compared to the resilience of society against these threats. All too often, even basic measures have still not been implemented sufficiently, such as the use of multi-factor authentication and reliable backup systems. The NCSC notes major differences between various sectors and organisations when it comes to their digital resilience. Organisations

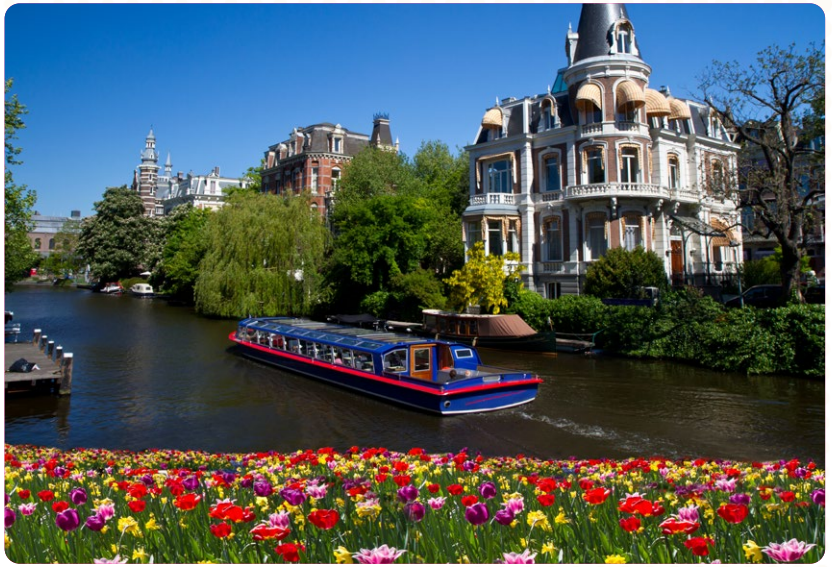


Photo by Luca Santilli on Shutterstock

that are sufficiently resilient have not only implemented basic security measures but have also focused on a risk-based method of working.

In order to resist cybersecurity threats, the Digital Trust Centre (DTC) was founded in December 2020 to help increase the resilience of businesses against digital threats. Also, the NCSC joined the so-called LDS, a platform in which both public and private parties, the NCSC and the DTC exchange information and knowledge about cybersecurity. This cooperation supports a more intensive information exchange between the NCSC and affiliated parties. Aside from the NCSC, there is also the National Coordinator for Security and Counterterrorism (NCTV). This government agency was established in 2012. Its aim is to protect Dutch society against disruptive security threats. NCTV monitors and coordinates initiatives from the public, private and public–private sectors to strengthen cybersecurity in the Netherlands. Cooperation between the General Intelligence and Security Service, the Dutch Military Intelligence and Security Service, the NCSC, the police and the public prosecutor has also been further strengthened. Additionally, the Dutch government appointed its first

Secretary of State for Digitalisation in January 2022, whose agenda for 2023 includes topics such as the improvement of digital literacy, combatting the spread of disinformation and the development of a quality mark for algorithms.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

Companies are well advised to conduct thorough due diligence on a target's IT environment and previous experience with security incidents, which should be logged internally as a requirement of law under the GDPR. The occurrence of a security incident need in itself not be worrisome. The response of the company to the incident can be much more telling about the company's readiness and level of compliance.

When it comes to privacy and personal data, we note an increased emphasis on compliance in the context of due diligence for M&A deals. This increased emphasis is evident in various different ways. First, target companies are investigated with more scrutiny for their GDPR compliance. Second, more thought is given to the GDPR aspects of the transaction itself, such as resulting data transfers or changes to intended use of data. This, no doubt, has everything to do with the risk presented by the enormous fines that can be imposed under the GDPR for non-compliance.

There is also an increased awareness among competition authorities about the importance of vast collections of data and their potential monetary value, even if this is not necessarily reflected by equally large market shares. The Dutch competition and consumer rights authority has also highlighted the collection of data by online platforms as a potential source of market power and the Ministry of Economic Affairs and Climate Policy has suggested that upcoming mergers and acquisitions should be reviewed based on deal value instead of the historic turnover of the companies involved. It is also noteworthy that last year the Dutch parliament has agreed on a new act (Wet VIFO) regulating investments in critical sectors, such as energy, logistics, finance and sensitive technology. The act introduces a notification obligation and requires authorisation from the Dutch Ministry of Economic Affairs and Climate.

QUESTIONS

Quinten Kroes
quinten.kroes@brinkhof.com

Quinten Pilon
quinten.pilon@brinkhof.com

Brinkhof NV
Amsterdam
www.brinkhof.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

A thorough understanding of cyber threats and the capability to work with relatively new and untested legal regimes. This requires an open mind, curiosity and creativity, and sometimes a healthy dose of paranoia about the threats. It is also important for the lawyer to have a technical interest or background, to help in bridging the cultural divide between IT specialists and the legal and compliance teams.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

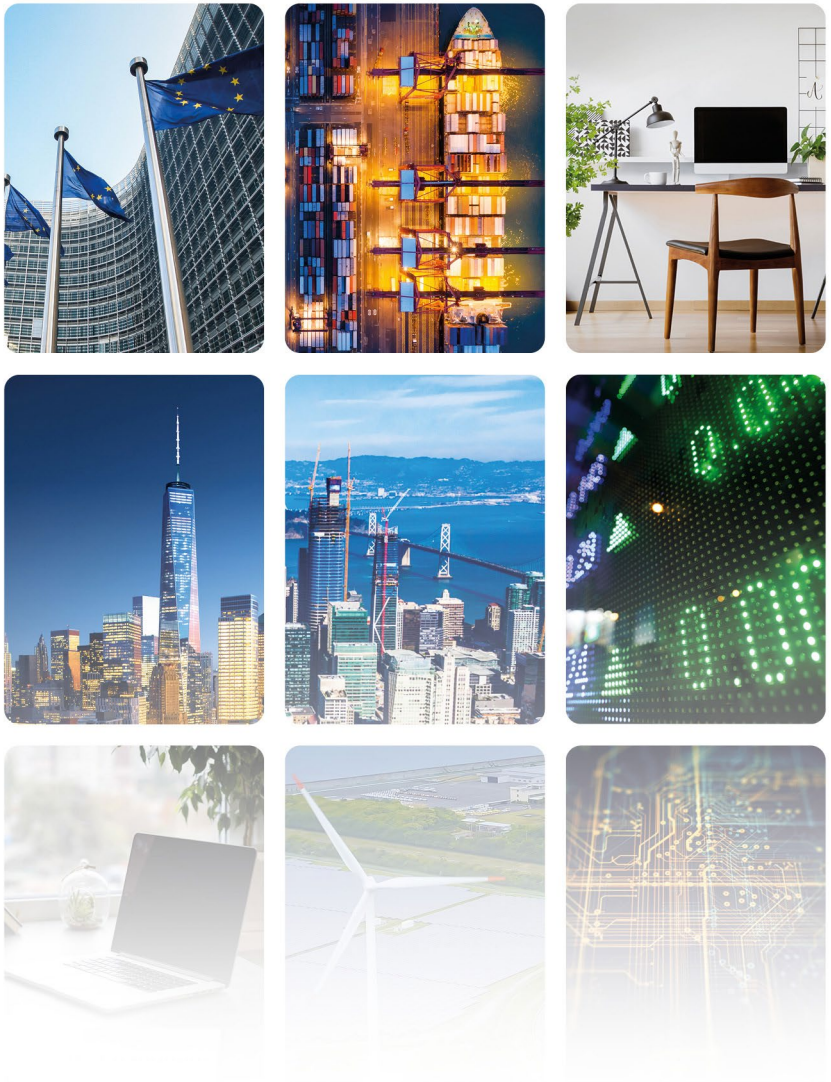
The Netherlands is a relatively tech-savvy country, with clients approaching us with innovative and challenging legal questions. Our data protection authority has also always taken a keen interest in new technical developments such as mobile apps, facial recognition software and Wi-Fi tracking in public spaces. It has taken aggressive stances on issues such as cookie consent and legitimate interests.

How is the privacy landscape changing in your jurisdiction?

The impact of the GDPR on the Dutch society is significant. Cybersecurity has become an increasing concern, and it has become a clear priority for the current government based on its coalition agreement. The Dutch DPA is also set to receive more funding. Aside from public enforcement, there is also a growing risk of private enforcement: the Netherlands is a venue of choice for GDPR-related collective damage cases.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

The Dutch DPA notes an increase in the amount of hacking, malware and phishing in the data breach notifications it receives. It therefore stresses the importance of using multiple factor authentication, and warns of malicious techniques such as social engineering, password spraying and credential stuffing. For its part, the NCSC continues to warn companies about the exploitation of VPN vulnerabilities by state actors and criminals.



About Market Intelligence

Respected opinion, expert judgement

Lexology GTDT: Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes in major jurisdictions around the world. Through engaging, easily comparable interviews, the series provides the legal profession's thought leaders with a platform for sharing their views on current market conditions and developments in the law.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most interesting cases and deals.

Read more Market Intelligence topics