PANORAMIC NEXT

Privacy & Cybersecurity

NETHERLANDS

LEXOLOGY

Privacy & Cybersecurity

2024

Cybersecurity continues to represent a growing risk for companies around the world, with cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime and 'hacktivists' continuing to grow on a global basis.

Generated: July 23, 2024

Netherlands

Quinten Kroes, **Quinten Pilon**, **Marije Rijsenbrij**
Brinkhof

Summary

PROFILES

About the lawyers

Q&A

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

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?

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

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

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

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

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

THE INSIDE TRACK

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

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

How is the privacy landscape changing in your jurisdiction?

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

Profiles

ABOUT THE LAWYERS

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's privacy and data protection team. He supports clients with queries across the full breadth of data protection and cybersecurity issues. Quinten specialises in data protection, TMT and competition.

Marije Rijsenbrij is an associate at Brinkhof's privacy and data protection team and specialises in data protection, TMT and platform regulation. She supports clients with queries across the full breadth of data protection and cybersecurity issues.

Q&A

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, in line with the objective of countering cyberthreats from foreign states, the Temporary Cyber Operations Act was approved in March 2024. When this Act comes into effect, it will allow the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) to more quickly and effectively act against threats from states that launch cyberattacks against the Netherlands. The Act provides, inter alia, an independent legal basis for cable reconnaissance and allows bulk datasets to be used for a longer period of time. This extension of the powers of the Dutch Intelligence Services is accompanied by a shift from prior review to binding supervision by the Commission Supervision Intelligence and Security Services (CTIVD) during the exercise of these powers.

Furthermore, the proposal for the Business Digital Resilience Promotion Act (Wbdwb) has passed the Dutch House of Representatives and is now before the Senate. This Act aims to provide non-vital businesses with general and specific information on cyberthreats and incidents.

At the European level, the NIS 2 Directive entered into force. This much-discussed legislation has widened the scope of the first NIS Directive and introduced key changes, including the size-cap rule, detailed rules for incident-reporting, stricter enforcement requirements, the harmonisation of sanction regimes across member states and improvement of cooperation. In the Netherlands, the draft NIS 2 Implementation Act was published for consultation on 21 May 2024. The Dutch government has stated that the NIS 2 implementation deadline of 17 October 2024 is unlikely to be met. The Act designates the Minister of Justice and Security as the central point of contact for NIS 2 matters and as

‘cyber crisis management authority’. The Dutch government has already provided online tools and a road map to help organisations assess whether and to what extent they are in scope of NIS 2 and to help them conduct a risk assessment.

Another landmark European cybersecurity act is the Digital Operational Resilience Act (DORA). This regulation creates a firm regulatory framework for digital operational resilience in the financial sector, by introducing rules for the protection against and the detection, containment and recovery from ICT-related incidents. Importantly, DORA applies not only to financial institutions, but also to non-financial service providers that provide third-party ICT services to financial institutions. The DORA is a lex specialis in relation to the NIS 2 Directive. The DORA is accompanied by the Digital Operational Resilience Directive, which should be implemented in national legislation by 17 January 2025, at the same time as the DORA provisions become applicable. The Dutch DORA Implementation Act, which implements DORA and the Directive, is now pending in the Dutch House of Representatives and includes amendments to bring the Financial Supervision Act (Wft) in line with the EU legislation.

Other notable updates to the EU cybersecurity landscape are as follows.

- The Cyber Resilience Act (CRA) is almost finalised after the Parliament approved the Act on 12 March 2024. The Council still needs to formally adopt the Act in order for it to enter into force. The CRA introduces mandatory cybersecurity requirements for a wide range of products with digital elements, including hardware, software and ancillary services. The cybersecurity standards that products must meet will depend on the risk associated with the product.
- The European Commission launched its first EU-wide cybersecurity certification scheme under the Cybersecurity Act in January 2024. The European Cybersecurity Scheme on Common Criteria (EUCC) provides rules and procedures for certifying ICT products throughout their life cycle, making products more reliable for users.
- Finally, in March 2024, a political agreement was reached between the European Parliament and the Council on the Cyber Solidarity Act. This Act introduces three measures: (1) a European Cybersecurity Alert System; (2) a Cybersecurity Emergency Mechanism to improve preparedness and response to significant and large-scale cyber incidents; and (3) a European Cybersecurity Incident Review Mechanism to review and assess important or large-scale incidents.

Aside from these new laws, the main regulatory development has been that the enforcement of the GDPR through collective class action claims is steadily increasing. As at May 2024, class actions have been started against many major tech companies, including Meta, Google, Amazon, Adobe, Salesforce and Oracle.

Finally, it is worth noting that in December 2023, Uber was fined €10 million by the Dutch DPA for insufficient compliance with information obligations (articles 12 and 13 GDPR). This was (by far) the largest fine ever imposed by the Dutch DPA. The fine followed a complaint to the French DPA, which forwarded the complaint to the Dutch DPA because Uber's European headquarters are in the Netherlands. Last year the Dutch DPA also fined credit card company International Card Services BV €150,000 for failing to perform a Data Protection Impact Assessment.

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 inform the data subjects (article 34 GDPR). This notification is not required if the controller has taken measures to ensure that the risk of a breach is unlikely to materialise.

Available guidance makes it clear that a number of criteria are relevant in assessing whether a notification is required, such as the sensitivity of the data, the number and vulnerability of data subjects affected, the volume of data lost and the potential impact on the data subjects.

In 2023, the EDPB conducted a thematic case digest that provides an overview of decisions adopted under the one-stop-shop procedure on security of processing and data breach notifications. Interestingly, the EDPB report found that data controllers tend to notify data breaches in most cases in order to avoid the risk of a GDPR infringement.

The Dutch DPA has stipulated the importance of notifying data breaches in the context of cyberattacks. According to the Dutch DPA, the risks of cyberattacks are often underestimated. The Dutch DPA emphasises that this type of data breach must almost always be reported to the Dutch DPA and the affected data subjects, especially when large amounts of data – or sensitive data – are involved, such as identification documents and credit card details.

The Dutch DPA has also provided guidance on whether ransomware can be considered a notifiable breach. In line with the EDPB's position, it takes the position that this is the case. It has also 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 the Dutch DPA or to the data subjects. After all, paying a ransom does not guarantee that hackers will actually delete all personal data (and not resell it).

The Dutch DPA occasionally launches investigations after large data breaches. In the past year, the Dutch DPA has monitored Booking.com after indications that Booking.com did not always report data breaches in a timely manner. In 2021, the Dutch DPA fined Booking.com €475,000 for failing to report a data breach in a timely manner. When conducting investigations, the Dutch DPA has can request information from the party that has suffered a data breach. However, in a recent ruling, the court held that the Dutch DPA could not request this information from a third party (in this case, the Dutch DPA was requesting information from a cybersecurity company about one of its customers). The Dutch DPA had to first try to contact the party that suffered the data breach, and only then could it request information from a third-party.

If in doubt, the Dutch DPA recommends making a preliminary notification of a possible breach. The notification can always be amended or even withdrawn at a later date, when the controller has more knowledge about the breach and its consequences. Controllers can make a notification via a web-based notification tool on the Dutch DPA's website. Although this tool is currently only available in Dutch, English submissions are now also accepted.

An English questionnaire containing all the questions of the online notification tool and some explanatory comments is also available on the website of the Dutch DPA.

WHAT ARE THE BIGGEST ISSUES THAT COMPANIES MUST ADDRESS FROM A PRIVACY PERSPECTIVE WHEN THEY SUFFER A DATA SECURITY INCIDENT?

When an incident occurs, organisations should prioritise remediation of the specific security issue and do their utmost to mitigate the negative consequences of the breach.

The measures to be taken will vary depending on the nature of incident, from attempting to locate a lost data carrier, to remotely wiping a portable device or working with a processor to determine the extent of a security incident in their domain.

Enforcement action by the Dutch DPA shows that proactive action following a data security incident can significantly reduce a fine following a security incident. The Dutch DPA fined a local bank for a data breach caused by poor identity verification by the telephone helpdesk, but later significantly reduced the fine from €310,000 to €150,000. It took into account the fact that the bank had compensated the affected individuals and provided the Dutch DPA with a comprehensive risk inventory and action plan. On its own initiative, the bank swiftly implemented a large number of improvement measures in its recording practices, system support, testing and assurance, and increased its internal professionalism and awareness in this area.

A data breach may indicate that existing organisational and technical measures are not adequate. Maintaining appropriate and adequate levels of security requires continuous effort and constant review through risk assessments, planning, execution, checking and doing the same all over again (the 'plan-do-act-check' cycle).

If an organisation suffers from a personal data breach because it has failed to comply with any of the GDPR's (security) obligations, individuals can claim compensation for the material and immaterial damage they have suffered. The CJEU has confirmed that the right to compensation is not limited to immaterial damages that reach a certain threshold of seriousness. At the same time, a mere infringement of the GDPR is not enough to claim compensation. Individuals must be able to demonstrate that they suffered actual damage as a result of an infringement. Furthermore, the CJEU has confirmed that the right to compensation is purely compensatory in nature (and not punitive). This also means that the severity of the infringement should not be taken into account for the purposes of compensation.

Dutch courts have granted several claims for damages over data breaches, although the amounts awarded are relatively modest. One aspect that courts seem to take into account when assessing claims for damages is the sensitivity of the personal data involved in the data breach. For example, a Dutch university has had to pay a student €300 after a hacker gained access to medical information.

Recently, a class action lawsuit was brought against the Dutch public health service after it suffered a massive data breach in which covid-19 test and trace data were leaked.

Note that the CJEU confirmed that a data security incident does not automatically indicate that an organisation has failed to take appropriate technical and organisational measures to protect personal data (in breach of the GDPR's security obligations). It is impossible to completely eliminate the risk of a data breach. The CJEU has also confirmed that

organisations will not be liable for damages if they are able to prove that they are in no way responsible for the event causing the damage, which may be the case where a data breach was caused solely by a third party.

WHAT BEST PRACTICES ARE ORGANISATIONS WITHIN YOUR JURISDICTION FOLLOWING TO IMPROVE CYBERSECURITY PREPAREDNESS?

Statistics by the National Cyber Security Centre (NCSC) show that the vast majority of cyberattacks are phishing, ransomware and distributed denial-of-service (DDoS) attacks, all of which require very different responses. To help organisations lay the foundations for effective cyber resilience, the NCSC has published eight basic security measures that organisations should implement.

Measure (1) is that organisations are advised to establish a risk management process that includes regular risk assessments to identify specific threats and determine which key assets need to be protected. In addition, (2) organisations should implement strong authentication and (3) ensure (role-based) access control to their data and services. Organisations are becoming increasingly aware that the implementing strong passwords alone is an outdated security mechanism. Password strength alone provides limited protection against phishing attacks. Therefore, both the NCSC and the Dutch DPA stress the importance of implementing multi-factor authentication.

Measure (4) is that organisations are also advised to ensure that their applications and systems generate sufficient log information. In this context, the NCSC recommends centralising log information and using automated log analyses. In the Netherlands, a hospital has had to pay €2,000 in damages for unauthorised access to medical records by an employee and for failing to monitor log files in a systematic and consistent manner.

Other basic measures include: (5) segmenting networks and limiting unnecessary functionalities of software, hardware and network equipment; (6) encrypting data as much as possible; (7) making necessary backups at different locations; and (8) setting up a patch management process to ensure the prompt identification, testing and installing of software updates.

Recently, the NCSC has also been raising awareness of supply chain risks. Small and medium-sized enterprises (SMEs) are increasingly targeted by supply chain attacks, due to weaker cybersecurity practices and limited resources. These attacks can disrupt the SME's operations and potentially trigger larger attacks on their partners. The NCSC has published a detailed best practice guide on how to manage supply chain risks. To manage supply chain risks, it is essential that organisations have clear agreements with their suppliers and subcontractors on mutual processes. A recent court case illustrates the importance of this. The court ordered a processor to provide detailed information about security incidents after it failed to do so in response to legitimate customer requests.

Note that the NIS 2 Directive also contains a duty of care that requires organisations to carry out their own risk assessment and, on the basis of that assessment, to take appropriate measures to secure their services as far as possible and to protect their network and information systems. This duty focuses on digital risks, including supply chain risks. Under the NIS 2 Directive, the governing bodies of in-scope entities must approve and oversee the implementation of cybersecurity risk management measures and, in certain

circumstances, may even be held liable for breaches of cybersecurity risk-management obligations.

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 remains responsible and liable for all personal data it collects or processes.

The Netherlands is a key player in the global digital infrastructure, acting as a major hub for internet traffic. A significant amount of international internet traffic passes through the Netherlands, thanks to the many submarine cables that land on its shores. This strategic position highlights the Netherlands' essential role in maintaining and securing global internet connectivity and has made the Netherlands an attractive destination for data centre investment. Recently, however, data centres have faced hurdles in setting up operations in the Netherlands due to spatial planning and energy supply issues. The challenges are compounded by the emergence of AI, which is increasing the demand for computing resources and data storage.

Under the GDPR, personal data may only be processed outside the European Union (more specifically, the European Economic Area (EEA)) if the third country in which the data is processed provides an adequate level of protection. Compliance can be achieved in a number of ways, all of which have to do with ensuring that adequate safeguards are in place, either within the company or in the country to which the data is transferred.

Since the adoption of the EU–US Data Privacy Framework (DPF), organisations have been able to transfer personal data from the EU to US companies participating in the DPF, without having to put in place additional privacy safeguards. Critics have raised concerns that the DPF is not sufficiently in line with the Schrems II- criteria, leaving the DPF vulnerable to a new legal challenge. For transfers of personal data to US companies that do not participate in the DPF, or to companies in other non-EEA countries where no adequacy decision has been made, the primary method is to use standard contractual clauses (SCCs), together with individual transfer impact assessments (TIAs). If the outcome of the TIA is the third country's laws and practices affect the effectiveness of the GDPR transfer mechanism, organisations will need to identify and implement additional measures to bring the level of protection for the personal data transferred up to the EU's level of protection.

The use of cloud hosting must be part of the overall risk assessment that the controller makes before moving to the cloud, which may require a data protection impact assessment under the GDPR. The Dutch government and Dutch educational organisations have commissioned various DPIAs on their 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 have guided the government's and educational institutions' negotiations with a number of large international cloud providers such as Microsoft, Google and Zoom.

HOW IS THE GOVERNMENT IN YOUR JURISDICTION ADDRESSING SERIOUS CYBERSECURITY THREATS AND CRIMINAL ACTIVITY?

In the Cybersecurity Assessment Netherlands (CSAN) 2023, the NCSC and the National Coordinator for Counterterrorism and Security (NCTV) concluded that digital risks to Dutch national security remain high. The most serious threats come mainly from state actors, cybercriminals and outages. However, the threat is constantly changing, for example due to geopolitical polarisation and Russia's war against Ukraine. Hacktivism has also come to the fore. The CSAN urges organisations to 'expect the unexpected'. One of the reasons for this call is the new threats posed by new technologies such as AI.

Last year, the Dutch government presented its new international cyber strategy for 2023–2028. The government has identified three key priorities for the coming years: (1) countering state and criminal cyberthreats; (2) strengthening democratic principles and human rights online; and (3) maintaining a globally connected, open, free and secure internet.

Steps are also being taken to merge three government cybersecurity organisations into one. This new central organisation will bring together the NCSC, the Digital Trust Centre (DTC) and the Computer Security Incident Response Team for Digital Service Providers (CSIRT-DSP). By 2026, the new organisation will be responsible for sending out cyberthreat alerts to organisations and will act as the government's single point of contact for reporting cyberthreats and seeking advice on cybersecurity.

Finally, in 2023, the Dutch DPA has launched a project with the Central Bureau of Statistics (CBS) to make information from data breaches reported to the Dutch DPA available for scientific and statistical research for (improving) cyber resilience.

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 not in itself be a cause for concern; the company's response to the incident can be much more indicative of the company's preparedness and level of compliance.

When it comes to privacy and personal data, we are seeing an increased focus on compliance in M&A due diligence. Target companies are investigated with more scrutiny for their GDPR compliance and more thought is being given to the GDPR aspects of the transaction itself, such as resulting data transfers or changes to the intended use of data. This is largely due to the risk of huge fines for non-compliance under the GDPR. However, under the banner of data protection compliance, regulators are also becoming increasingly involved in issues concerning companies' business practices. For example, in April 2024, the EDPB issued an opinion rejecting Meta's new consent-or-pay model.

There is also a growing awareness among competition authorities of the importance of vast collections of data and their potential market power or monetary value, or both, even if this is not necessarily reflected by equally large market shares.

In addition, there is an increased focus on the regulation of foreign direct investment (FDI) in the Netherlands. In the summer of 2023 a new FDI Act entered into force (Wet VIFO), regulating investments in providers of essential services (eg, financial services, energy and transport) and companies that are active in the field of sensitive technologies. The

Wet VIFO introduces a notification obligation and requires authorisation from the Dutch Ministry of Economic Affairs and Climate.

The Inside Track

WHEN CHOOSING A LAWYER TO HELP WITH CYBERSECURITY, WHAT ARE THE KEY ATTRIBUTES CLIENTS SHOULD LOOK FOR?

Clients should prioritise expertise in data protection laws, a thorough understanding of cyberthreats and the ability 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. Look for a track record of dealing with cyber incidents, strong problem-solving skills and the ability to navigate complex regulatory environments. A technical background or interest is essential to bridge the cultural gap between IT specialists and legal teams.

WHAT ISSUES IN YOUR JURISDICTION MAKE ADVISING ON CYBERSECURITY AND PRIVACY COMPLEX OR INTERESTING?

The Netherlands is a relatively tech-savvy country, and clients come to us with innovative and challenging legal questions. The Dutch DPA is known for its proactive stance and strict enforcement of the GDPR. It has always taken a keen interest in new technological developments such as the emergence of generative AI. This is reflected in the fact that the Dutch DPA now also acts as the National Coordinating AI Supervisor, a coordinating role to improve cooperation between Dutch regulators. The Dutch government has also taken a proactive stance on AI and is one of the first EU member states to publish a government-wide vision on generative AI.

HOW IS THE PRIVACY LANDSCAPE CHANGING IN YOUR JURISDICTION?

The intersections between consumer protection, privacy, and competition law enforcement are becoming more apparent, as seen in the introduction of the Digital Services Act (DSA), the Digital Markets Act (DMA) and the involvement of privacy regulators in companies' (pay-or-okay) advertising business models. To improve enforcement in the digital sector, regulators cooperate through initiatives such as the Dutch Digital Regulation Cooperation Platform (SDT). In addition, the Netherlands has emerged as a key venue for GDPR-related collective damages cases against major tech companies, including Salesforce, Oracle and Google.

WHAT TYPES OF CYBERSECURITY INCIDENTS SHOULD COMPANIES BE PARTICULARLY AWARE OF IN YOUR JURISDICTION?

Ransomware continues to be a major component of cyberattacks. The Dutch DPA notes that data breaches caused by hacking, malware and phishing remain among the most frequently reported incidents. In addition, the NCSC is raising awareness about the risks posed by the interconnected nature of organisations. Cyber incidents can affect multiple organisations within this wider ecosystem. The Dutch DPA advises that organisations

should 'almost always' report cyberattacks due to the significant risks these data breaches pose to data subjects, including identity fraud and scams.

Brinkhof

Quinten Kroes quinten.kroes@brinkhof.com
Quinten Pilon quinten.pilon@brinkhof.com
Marije Rijsenbrij marije.rijsenbrij@brinkhof.com

Brinkhof