THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

EIGHTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADERS
Joel Woods, Jack Bagnall

BUSINESS DEVELOPMENT MANAGERS
Rebecca Mogridge, Katie Hodgetts, Joey Kwok

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Georgia Goldberg

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Jonathan Allen

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-810-9

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ADVOKAADIBÜROO NORDX LEGAL

ALLENS

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS & PARTNERS

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

K&K ADVOCATES

LEE, TSAI & PARTNERS

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 19

NETHERLANDS

Herald Jongen, Nienke Bernard and Emre Yildirim[1]

I OVERVIEW

Data protection and data security are key areas for our increasingly digital society and the digital transformation that organisations and their products, services and business models undergo. Both areas have seen significant legal development over the past years following the entry into force of key European legislation such as the General Data Protection Regulation (GDPR) and the Security of Network and Information Systems Directive (the NIS Directive).

The GDPR applies in the Netherlands, as supplemented by the General Data Protection Regulation Implementation Act (the Dutch Implementation Act) and various sector-specific legislation relating to the processing of personal data.

This chapter provides a pragmatic overview of the current legal landscape in the Netherlands and related key legal developments over the past year, including enforcement actions by the Dutch Data Protection Authority (the Dutch DPA).

II THE YEAR IN REVIEW

2020 and 2021 have again been a busy period in the Netherlands, with data protection- and security-related news frequently being the subject of press coverage and public discussion. Major incidents such as a breach of the Dutch health authorities' covid-19 systems, exposing data of thousands of Dutch citizens, have been widely covered by the media. Furthermore, in June 2021 the Dutch DPA advised against schools and other educational institutions using Google G Suite for Education (now rebranded to Google Workspace for Education) as of August 2021, because of high data protection risks identified in data protection impact assessments (DPIAs) commissioned by the Dutch government and by the main educational organisations (SURF and SIVON), of which most schools and universities are a member. This led to emergency negotiations between SURF, SIVON, the Dutch government and Google, during which a remediation plan was agreed, and the use of Google products can be continued.[2]

The Dutch DPA faced the harsh reality of its insufficient budget, leading to a high workload and ultimately resulted in the Dutch DPA not being able to properly carry out its tasks. While the Dutch DPA has requested an increase in its budget for years now, this year was a tipping point. In its annual report for 2020, the Dutch DPA describes the constraints

1 Herald Jongen is a shareholder and Nienke Bernard and Emre Yildirim are associates at Greenberg Traurig LLP.

2 All information can be found here: https://www.surf.nl/en/news/agreement-with-google-on-privacy-risks.

it is facing due to this bottleneck in a cry for help; these range from investigations not being initiated due to insufficient resources and data subjects (and data controllers alike) not being helped in a timely manner (or at all). The Dutch DPA's request for more resources has been successful this time: Parliament voted in favour of a motion to significantly increase the budget of the Dutch DPA.

Enforcement by the Dutch DPA is often initiated following complaints made by data subjects, current affairs brought to public attention by politicians, or the results of investigative journalism. Data subjects continue to find their way to the Dutch DPA with complaints. In its annual report for 2020, the Dutch DPA notes that it received almost 26,000 complaints from individuals.[3] The Dutch DPA notes that most complaints concerned a violation of a data subject's right, such as the right of access and the right to erasure. Organisations are, therefore, recommended to implement robust data subjects' rights processes and handle requests with due care.

In its agenda for 2020–2023, the Dutch DPA has specified that it will be focusing enforcement efforts specifically on data brokering and the use of artificial intelligence and algorithms.[4] Within data brokering, the Dutch DPA will focus most strongly on the internet of things, where it hopes to increase use of standards and certification, and profiling, where it will focus on enforcement and behavioural advertising stimulating the creation of codes of conduct and enforce it actively. The call for supervision of AI and algorithms is increasing among politicians and in Dutch society. Within AI, the key focus will be the development of a regulatory framework that the Dutch DPA will use for its supervision of AI. In February 2020, the Dutch DPA published its vision for enforcement relating to AI.[5]

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The processing of personal data in the Netherlands is primarily governed by the GDPR and the Dutch Implementation Act, which includes exemptions and limitations as allowed by the GDPR.[6] Examples of where the Dutch Implementation Act deviates from the GDPR include additional conditions relating to the processing of genetic data, biometric data, data concerning health and criminal convictions and offences, and exemptions to data subjects' rights obligations in certain specific cases as discussed throughout this chapter.

In July 2020, a public consultation was concluded for the prospective Data Protection Collective Act. The Act's purpose is to amend the Dutch Implementation Act, and update various Dutch laws to promote further consistency with the GDPR. Proposed amendments include further specification of conditions under which biometric data may be processed and an exemption to the prohibition to process special categories of personal data if the processing is necessary for an audit required by law to be performed by an accountant. The Act is still subject to the legislative process and is expected to enter into force in 2021.

3 https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf.

4 https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/focus-ap-2020-2023.

5 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/toezicht-op-algoritmes.

6 Available at https://wetten.overheid.nl/BWBR0040940/2020-01-01.

As further discussed below under specific regulatory areas, various sector-specific laws also provide rules on the processing of personal data (e.g., in the financial, telecoms and healthcare sectors).

ii General obligations for data handlers

The main obligations of controllers and processors are set out in the GDPR. From time to time, the Dutch DPA issues guidance on specific aspects of the GDPR and data protection in general. In July 2021, for example, the Dutch DPA published guidance on cross-sectoral blocklists and the position of DPO in an organisation.[7] The Dutch DPA has a strict view on the use of legitimate interest as a legal ground: merely serving purely commercial interests, profit maximisation, following the behaviour of employees without (legitimate) interest or the (buying) behaviour of (potential) customers do not constitute legitimate interests. This point of view seems stricter than that of other supervisory authorities and previous guidance by the Article 29 Working Party. While this form of guidance from the Dutch DPA is not legally binding, the Dutch DPA will likely take this interpretation into account in its supervisory and enforcement decisions. The Dutch DPA did receive a first blow on its strict views on legitimate interest by a Dutch court. The District Court Midden Nederland ruled that if an envisaged interest is not illegitimate or against relevant laws, it qualifies as a legitimate interest under the GDPR. In this respect, it does not matter whether this interest is of a commercial nature. A fine imposed by the Dutch DPA on VoetbalTV of €575,000 was annulled by the court. It is yet to be seen whether the Dutch DPA will stick to or revise its strict views.

iii Data subject rights

Pursuant to Chapter III of the GDPR, data subjects have the right to access, rectification, erasure, restriction of processing, data portability, object and to not to be subject to a decision based solely on automated processing, including profiling. The Dutch Implementation Act provides exemptions to data subject rights for all matters set out in Article 23(1) GDPR. Other exemptions apply when processing solely for journalistic purposes or for the benefit of academic, artistic or literary expression forms, automated decision-making (excluding profiling) if necessary for the compliance with a legal obligation or the performance of a task carried out in the public interest. Finally, the right to object does not apply to public registers established by law, and the right to access, rectification and restriction are not applicable to public registers provided that special procedures are established with respect to these rights by other laws.

The right of access is the most exercised right and is used for various purposes, including pseudo-discovery in legal proceedings, often in the context of employment disputes.

iv Specific regulatory areas

In addition to the GDPR, various sector-specific laws and regulations contain rules relating to the processing and security of data. These include:

a telecoms: the processing of traffic and location data under the Telecommunications Act;

7 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-duidelijkheid-over-zwarte-lijsten-delen-met-andere-sectoren and https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-uitgangspunten-voor-inrichten-sterk-intern-toezicht.

b healthcare: the processing of personal data concerning health under the Medical Treatments Contracts Act and the Act on Additional Provisions for the Processing of Personal Data in Healthcare;

c energy: the processing of personal data relating to energy use, including smart meters, under the Electricity Act and Gas Act and related subsequent legislation;

d law enforcement and judiciary: such as the processing of personal data under the Act on Police Records and the Judicial Data and Criminal Records Act; and

e financial institutions: as further discussed below.

v Financial sector

Many rules applicable to financial institutions originate from EU law, either directly (such as MiFIR) or via implementation of directives such as CRD IV and AMLD into the Financial Supervision Act and the Money Laundering and Terrorism Financing Prevention Act and subsequent regulations. These regulations contain a wide range of data and security related topics, such as retention and reporting obligations under MiFID II/MiFIR, requirements relating to cloud outsourcing under the EBA guidelines and obligations to use two-factor authentication under PSD II. The Financial Supervision Act mandates extensive policies and procedures with respect to business continuity, disaster recovery and information security that are generally applicable to all regulated financial undertakings, including consumer credit providers and advisers and offerors of financial products.

Credit institutions, operators of trading venues (regulated markets, MTFs and OTFs) and central counterparties are designated as essential services providers under the NIS directive (as implemented into Dutch law) with respect to the offering and settlement of payment and securities transactions. Incident notification obligations under the Security of Network and Information Systems Act generally apply in addition to incident notification requirements under the Financial Supervision Act and the GDPR. With respect to data breaches under the GDPR, the Dutch Implementation Act stipulates that financial undertakings that are subject to the Financial Supervision Act are exempted from the obligation to communicate personal data breaches to data subjects.

Information and cybersecurity and use of (client) data are important topics in the supervisory policies of the financial regulators Authority for the Financial Markets and the Dutch Central Bank. Both supervisors regularly publish guidance and good practices, such as the 'Principles of Information Security' from the Authority for the Financial Markets and the 'Information Security Monitor' from the Dutch Central Bank.

vi Public registers

In certain specific situations, Dutch law provides that personal data must be included in public or semi-public registers. Examples are the Dutch Credit Registration Bureau, the registers for board and supervisory board members of certain financial institutions with the Authority for the Financial Markets and registers of the Employee Insurance Agency. In addition, the register of the Chamber of Commerce may include personal data relating to a person's business or employment. In addition, effective 27 September 2020, most Dutch non-listed companies are required to register their ultimate beneficial owners (UBOs) with the Chamber of Commerce. This obligation under the UBO Register (Implementation) Act follows from the AML Directive. The UBO register will be public, but the Chamber of Commerce may be requested to protect the identity of the UBO in special circumstances, for example if the shareholder is a minor or has police protective security.

vii Covid-19

The covid-19 pandemic has reignited attention to workplace privacy as the pandemic introduced a need for organisations to process personal data (including data concerning health) in light of the challenges brought by the pandemic. Such challenges include the processing of health data of employees or visitors, secure remote working and videoconferencing.

In March 2020, the Dutch DPA first communicated a lenient approach on enforcing data protection obligations during the pandemic, enabling organisations to focus their resources on combating the pandemic. Later in 2020 a more stringent approach started, where the Dutch DPA initiated enforcement actions against two companies regarding the unlawful processing of health data of employees.[8] Throughout the pandemic, the Dutch DPA has actively published guidance on various topics, including:

a privacy aspects of videoconferencing apps;
b secure remote working;
c the permissibility of temperature checks of employees and visitors;
d anonymity of aggregated telecommunication data; and
e contact tracing apps.

viii Technological innovation

Internet of things

Given the rise in the use of smart devices and connected cars, it is not surprising that the internet of things is a key focus area in the enforcement agenda of the Dutch DPA. In particular, the Dutch DPA voiced concerns about the security of smart devices and the detailed view of an individual's personal life that the collected data may give. In June 2019, the Dutch DPA published practical guidance for data subjects relating to the purchasing, installation and use of smart devices.[9] In March 2020, the Dutch DPA published practical guidance for data subjects on the purchasing, using, selling and renting of connected cars.[10] In July 2021, the Dutch DPA published a report regarding the development of smart cities in the Netherlands.[11]

Biometric data

Following signs that supermarkets were interested in using facial recognition, the Dutch DPA reminded supermarkets of the rules for facial recognition in a letter published in June 2020.[12] By providing information and intervening where necessary, the Dutch DPA intends to prevent supermarkets from unlawfully using facial recognition. In December 2020, the Dutch DPA issued a formal warning to a supermarket due to unlawful use of facial recognition.[13] A related interesting development is the use of artificial intelligence and machine learning to create deepfakes: fabricated media in which an individual in an existing image or video is replaced with another individual's likeness.

8 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-onderzoekt-meten-temperatuur-werknemers-tijdens-corona.
9 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-tips-voor-privacy-bij-internet-things-apparaten.
10 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-tips-voor-privacy-bij-connected-cars.
11 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-aanbevelingen-voor-smart-cities.
12 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-wijst-supermarkten-op-regels-gezichtsherkenning.
13 https://autoriteitpersoonsgegevens.nl/nl/nieuws/formele-waarschuwing-ap-aan-supermarkt-om-gezichtsherkenning.

Cookies

In the Netherlands, the use of non-strictly necessary cookies and similar technologies is generally subject to explicit consent under the Telecommunications Act. Cookie compliance continues to be of interest to the Dutch DPA and the Authority for Consumer and Market. In December 2019, the Dutch DPA published the outcome of an investigation into the use of tracking cookies.[14] Of 175 websites, half utilised tracking cookies without meeting consent requirements. The Dutch DPA stressed that the following methods of obtaining consent for tracking cookies are non-compliant:

a omission to indicate preferences or inactivity;
b further navigating throughout the website; or
c pre-checked boxes.

The Dutch DPA also reiterated its position that websites that only provide access if they consent to placing tracking cookies (cookie walls) are not compliant with the GDPR as they do not provide data subjects a free choice. In 2020, the Dutch DPA investigated the use of cookie walls and tracking cookies at various organisations.

Data ownership and control

Under Dutch law, the concept of 'ownership' only applies to tangible assets and is therefore not applicable to the automated processing of (personal) data. Data may be protected by data protection laws, intellectual property rights and contractual terms. A party that wants to be – and more importantly stay – in control of its data must therefore use data protection laws to its advantage and negotiate terms that not only comply with any requirements under the GDPR, but also enable it to be and remain in control of its data.

There is an increasing trend of discussions between customers and cloud providers regarding their data protection roles under the GDPR, particularly with respect to metadata. In 2020, following negotiations with the Dutch government in 2019, Microsoft was the first cloud provider to change its general terms for enterprise customers and internal processes, adopting a processor role for almost all personal data processed in the context of its online services. In 2020, the Dutch government commissioned a DPIA on Google Workspace and on the basis thereof negotiated with Google about GDPR-compliant use of Google products and services.[15] These negotiations resulted in a prior consultation of the Dutch DPA (on the basis of Article 36 Paragraph 1 GDPR). This consultation led to the advice in June 2021 not to start using Google products until the high risk identified in the DPIA is remedied.[16] It is expected that on the basis of this advice (which resembles the advice of the Dutch DPA not to use Google for Education in schools, mentioned in Section II) the government and Google will reach agreement on a remediation plan by 1 January 2022.

14 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op-onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies.

15 https://slmmicrosoftrijk.nl/sdm_downloads/data-protection-impact-assessment-google-workspace/.

16 https://slmmicrosoftrijk.nl/sdm_downloads/google-workspace-advies-autoriteit-persoonsgegevens/.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

Under the Dutch Implementation Act, international data transfers to third countries or international organisations are generally not subject to restrictions beyond those set out in Chapter V (titled 'Transfers of personal data to third countries or international organisations') of the GDPR.

The Schrems II ruling continues to keep data controllers puzzled. On 16 July 2020, the European Court of Justice (ECJ) ruled in *In Schrems II* (*Schrems II*)[17] that the transfer of personal data from the European Union to the United States can – with immediate effect – no longer be based on the EU–US Privacy Shield framework. The standard contractual clauses for the transfer of personal data to processors in third countries (SCC) as adopted by the European Commission remain valid. However, the ECJ emphasises the responsibility of controllers, and in the alternative, supervisory authorities to assess on a case-by-case basis whether the SCC provide an adequate level of protection for a specific transfer. The ECJ explains that any assessment of an adequate level of protection must be based on the same elements that have led to the invalidation of Privacy Shield. The same criteria apply to other data transfers mechanisms under Article 46 GDPR, including binding corporate rules.

The assessment by the controller whether there is an adequate level of protection is not an easy one to make. Thorough and extensive research is necessary, in particular regarding the various US regulations, and the assessment by European and national courts and supervisory authorities will also have to be taken into account. Although the EDPB provided six-step recommendations on measures that data controllers and processor can take, the task at hand continues to be tough. Most very large enterprises have initiated some kind of investigation or assessment exercise in order to be able to prove that they have at least started the job, but also these controllers are anxiously waiting for guidance by the supervisors or new legislation,

SCC and binding corporate rules continue to be the data transfer mechanisms that are generally most relied upon by organisations. While binding corporate rules provide multinational organisations with a robust framework for international data transfers, it should be noted that the Dutch DPA has had a significant backlog on approving binding corporate rules for years. In its annual report of 2020, the Dutch DPA notes that it received 12 new binding corporate rules (BCR) requests and five BCR update requests. Owing to understaffing, the workload at the end of 2020 totalled 46 BCR requests and 26 BCR update requests. Organisations that are considering adopting BCR with the Dutch DPA as their lead authority should therefore take into account that formal approval of BCR may take longer than anticipated and in practice will likely take upwards of five years.

The Netherlands does not have any formal laws containing specific data localisation requirements. However, there is an increasing demand to keep (personal) data as much as possible within the European Union.

V COMPANY POLICIES AND PRACTICES

In the Netherlands, privacy policies are widely used to comply with the transparency obligations under Article 5 and Chapter III of the GDPR and are often published online. Most organisations have at least a basic privacy policy in place for clients and customers,

17 ECJ, Case C-311/18, 16 July 2020 (*Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems*).

while larger organisations generally implement more sophisticated policies and procedures, including employee data privacy policies and internal procedures relating to use and security (breaches) of data. In a number of cases, Dutch sector-specific legislation mandates the implementation of data and security related policies.

Employee training relating to data protection and security is more prominent in larger organisations and is mandatory in certain sectors, such as for financial institutions.

Larger organisations (more than 50 persons) are obligated to implement a whistle-blower policy pursuant to the House for Whistleblowers Act. Furthermore, organisations that have established a works council, which is usually mandatory except for small organisations, must obtain approval from the works council prior to the introduction or alteration of certain policies such as an employee privacy policy or policies relating to employee monitoring and attendance registration. A mandatory advice procedure applies with respect to the introduction or alteration of an important technological provision.

On 27 November 2019, the Dutch DPA published a list of processing activities that require a mandatory DPIA, such as employee monitoring, profiling and credit scoring, that applies in addition to the guidance of the EDPB. If a DPIA indicates that processing will result in high risk, the controller must take mitigating measures or, in the absence thereof, consult the Dutch DPA prior to the processing. In 2019, the Dutch DPA received eight requests for a prior consultation. We notice an increase in the publication of DPIAs performed by the public sector, such as the DPIAs of the Ministry of Justice and Security for (1) Microsoft's Windows 10 and Office 365; and (2) Google Workspace.[18]

With respect to codes of conduct under Article 40 GDPR, the Dutch DPA approved the code of conduct for IT companies from the sector organisation Nederland ICT.

VI DISCOVERY AND DISCLOSURE

Disclosure of personal data to third parties is generally subject to and must comply with the GDPR and the Dutch Implementation Act.

The Netherlands does not have extensive (pretrial) discovery of documents available in some countries such as the United States. Subject to strict conditions, the Dutch Civil Procedure Code does provide the possibility to apply for a court order to review, obtain an extract from or obtain a copy of certain specific documents in the possession of another party.

A controller will generally be able to base any intended disclosure following a court order or governmental request to disclose personal data on the legal ground of compliance with a legal obligation to which the controller is subject, provided that the request has a basis under Dutch, European Union or another member states' law and the controller has a binding legal obligation to respond to such request. Any disclosure of sensitive categories of personal data or personal data relating to criminal convictions and offences must additionally comply with, respectively, Articles 9 and 10 GDPR and the Dutch Implementation Act.

Governmental requests from and civil discovery procedures in countries outside of the European Economic Area that require disclosure of personal data can only be recognised or enforceable if the request is based on an international agreement between the third country and the European Union or the Netherlands. A mutual legal assistance treaty is expressly

18 https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise and https://www.rijksoverheid.nl/documenten/publicaties/2021/02/12/google-workspace-dpia-for-dutch-dpa.

recognised as such an international agreement. Transfers must also comply with other requirements regarding international transfers as described in Section IV, above. In practice, this can be difficult as third-country organisations are often reluctant to enter into standard contractual clauses. Depending on the circumstances of the case, organisations may be able to rely on the grounds for incidental transfers set out in Article 49 GDPR, such as the necessity for the establishment, exercise or defence of legal claims.

If an organisation cannot base a disclosure on a legitimate ground for transfers to third countries or successfully direct a requesting party to an available international agreement, they may find themselves fallen between two stools. In such cases, a risk-based assessment must be made with regard to potential sanctions faced by the organisation for (1) not complying with the request and (2) breaching data protection laws.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The Dutch DPA is the designated supervisory authority for the Netherlands. In the execution of its powers, the Dutch DPA is bound by the principles of proper administration and procedural rules of the General Administrative Law Act. The Dutch Implementation Act grants the Dutch DPA administrative enforcement rights, such as fines and orders on penalties. Organisations and individuals can object to, and appeal against, decisions of the Dutch DPA before administrative courts. The Freedom of Information Act applies to the activities of the Dutch DPA.

The Dutch DPA is not the only authority involved in the supervision of personal data processing and security. The Dutch DPA established cooperation protocols with other supervisory authorities such as the Authority for Consumers and Markets, the Dutch Central Bank and the Telecom Agency. These cooperation protocols outline, among others, how the supervisory authorities cooperate in the case of enforcement, which supervisory authority will engage in enforcement for specific topics and how they exchange information.

The Authority for Consumers and Markets is the supervisory authority charged with enforcement of consumer protection laws and sector-specific regulation of several sectors.

The Authority for the Financial Markets, European Central Bank and Dutch Central Bank supervise financial institutions and markets, including the strict laws relating to data security that apply in this sector. The Dutch Central Bank is also the supervisory authority for financial institutions that are designated as essential services providers under the Security of Network and Information Systems Act that implements the NIS directive.

While the Dutch DPA and the Authority for the Financial Markets currently do not have a cooperation protocol in place, both authorities participate in the Consultation Forum of Regulatory Bodies (*Markttoezichthoudersberaad*), where various supervisory authorities that (partly) focus on the functioning of markets and the behaviour of market players come together to share knowledge and exchange experiences on cross-curricular themes. Other participants include the Authority for Consumers and Markets and the Dutch Central Bank.

ii Recent enforcement cases

Despite its high workload, the Dutch DPA has initiated quite a high number of enforcement cases this year: 24 cases.

In last year's chapter, we noted that the popular China-based social media app TikTok was under investigation by the Dutch DPA .[19] The Dutch DPA had voiced specific concerns regarding the processing of personal data of children, as TikTok is widely used among them. The investigation resulted in the Dutch DPA imposing a fine of €750,000 on TikTok for violation of Article 12 GDPR: among others. TikTok only made an English privacy notice available to Dutch users, and thus Dutch children.[20]

Further interesting enforcement actions by the Dutch DPA include a fine of €475,000 imposed on Booking.com in March 2021 for a late notification (22 days) to the Dutch DPA of a data breach.[21] In April 2021, the Dutch DPA imposed a fine of €600,000 on the municipality of Enschede for unlawful WiFi tracking of individuals in the city centre.[22] The Dutch DPA found that the municipality had no valid legal ground for the processing and noted that the municipality has appealed the fine.

iii Private litigation

Dutch civil courts may award actual damages to data subjects if they are able to prove that damages have occurred as a result of a breach of data protection legislation. There is an increase in private enforcement of data protection obligations and data subjects have been and continue to be awarded damages in various civil cases.

An interesting development we noted last year was the entry into force of the Collective Damages in Class Actions Act in January 2020. This Act paved the way for class actions through Dutch courts, including for breaches of data protection legislation. Under the Act, an interest organisation may claim monetary damages for its members, provided that the action has a sufficiently close connection with the Netherlands.

In August 2020, the interest organisation Privacy Collective launched the first GDPR-related class action. The Privacy Collective is seeking damages from Oracle and Salesforces for the alleged unlawful processing of personal data of Dutch internet users by using third-party cookies for advertisement tracking and targeting. Since then, several class actions have been filed, including actions against Facebook and TikTok. We expect this trend of GDPR-related class actions finding their way through the Dutch courts to increase in the coming years.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

In line with the territorial scope of Article 3 of the GDPR, the Dutch Implementation Act applies to the processing of personal data as part of the activities carried out on behalf of a controller or processor established in Netherlands, regardless of whether the processing takes place in the Netherlands. Similarly, the Dutch Implementation Act applies to the processing of personal data of data subjects who are in the Netherlands by a controller or processor not established in the Netherlands, where the processing activities are related to:

a the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Netherlands; or

19 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-start-onderzoek-naar-tiktok.

20 https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-tiktok-vanwege-schenden-privacy-kinderen.

21 https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-bookingcom-voor-te-laat-melden-datalek.

22 https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-gemeente-enschede-om-wifitracking.

b the monitoring of their behaviour as far as their behaviour takes place within the Netherlands.

If a controller or processor to which the GDPR applies does not have an establishment within the European Union, it may be required to appoint a representative within the European Union pursuant to Article 27 GDPR. In addition to GDPR requirements, foreign organisations should be aware that strict rules apply with respect to consumer protection, online sales and use of cookies.

IX CYBERSECURITY AND DATA BREACHES

Cybersecurity continues to be a top priority. The SolarWinds and Kaseya attacks sent shivers down the spine of the security community due to its sophistication and widespread effects, which did not leave Dutch entities untouched. It once more became evident that state actors are growing their cyber-arsenal and do not shy away from employing such weapons. However, attacks by private actors should not be underestimated, and neither should the need for effective cybersecurity practices. This was painfully demonstrated in October 2020 by a Dutchman that discovered that the password for President Trump's Twitter account was 'maga2020!'

Organisations (including government entities and non-profit organisations) are subject to the security requirements for personal data set out in the GDPR, including data breach reporting requirements. In 2020, the Dutch DPA received about 24,000 notifications of data security breaches.[23]

Additional rules apply to government organisations and organisations in certain sectors such as healthcare and financial institutions. Mostly, requirements relating to data and cybersecurity are principle-based rather than rule-based, meaning organisations have some freedom in determining what measures to implement. However, in some cases, the law mandates the use of certain technologies or standards. Examples are DigiD, the identity management platform for communication between government organisations and Dutch residents, and mandatory NEN information security standards for the healthcare sector.

Best practices differ based on the size of the organisation as well as the risks involved. In addition to any mandatory legal requirements that may apply, organisations that process large amounts of data or sensitive data are expected to have robust policies in place and commitments in this respect (including audit obligations) are often the topic of negotiation in negotiations and included in contractual documentation. Increasing GDPR and security awareness and developments such as the *Schrems II* ruling and remote working due to the covid-19 pandemic continue to boost procuring market parties' critical view of security. Organisations hoping to do business in the Netherlands should take into account that information and cybersecurity, including mitigation of risks that can lead to a loss of control or foreign state access, can be a deal-breaker when not properly addressed.

Designated operators of essential services and digital services providers are subject to the Security of Network and Information Systems Act and secondary regulations, which implement the NIS Directive. The supervisory authority for these organisations is the Dutch Minister responsible for the sector that the relevant service provider operates in. Essential and digital service providers are obligated to maintain adequate technical and organisational

23 https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2020.pdf.

procedures and measures that mitigate security risks of network and information systems and prevent incidents. In the case of a threatened or actual incident, notification must be made to the relevant Computer Security Incident Response Team (CSIRT), which is the National Cybersecurity Institute for essential service providers and the CSIRT-DSP for digital service providers. In December 2020, the European Commission launched its EU Cybersecurity Strategy for the Digital Decade. A key legal development is the revised Directive on Network and Information Systems (the NIS Directive). The proposal addresses the deficiencies of the current NIS Directive and future-proofs it. The new NIS Directive will include new sectors and classify entities as essential (for the sectors of energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration and space), or important (for the sectors of postal and courier services, waste management, manufacture, production and distribution of chemicals, food production, processing and distribution, manufacturing and digital providers).

All medium and large enterprises (as defined under EU law) that operate within these sectors will fall within the scope of the revised Directive. Requirements are introduced that require management of in-scope entities to supervise security risk management measures and to set up security trainings. The new NIS Directive further expands reporting obligations and harmonised administrative fines up to the higher of €10 million or 2 per cent of the total worldwide annual turnover.

The National Cybersecurity Institute frequently publishes White Papers and guidance with respect to security measures. In cooperation with a Dutch university, the National Cyber Security Centre developed the 'Cyber Cube Method', a framework that combines European Union Agency for Cybersecurity (ENISA), National Institute of Standards and Technology and George Mason University requirements to identify the required competencies of Security Operations Centers and CSIRT personnel based on the services offered by the relevant organisation.

The appointment of a chief information security officer and policies regarding internal reporting lines are in some cases mandatory based on sector-specific rules, such as the Financial Supervision Act and ENISA guidelines for digital service providers. The Dutch Corporate Governance Code, applicable to Dutch listed companies on a 'comply-or-explain' basis, requires the management and supervisory boards to have sufficient expertise to identify opportunities and risks that may be associated with innovations in business models and technologies in a timely manner, and to implement adequate risk-management policies. In its report on the financial year 2018, the Monitoring Committee Corporate Governance Code identified that most companies view cybersecurity as an operational risk and urge companies to (also) consider this risk in the context of long-term value creation of the company, which is one of the basic principles of the Corporate Governance Code.

A notable public initiative that we noted last year is the Dutch Institute for Vulnerability Disclosure (DIVD), an organisation of information security experts committed to reporting vulnerabilities they find in digital systems to people who can fix them. This institute played a key preventive and reactionary role in identifying the vulnerabilities that were used for the sophisticated Kaseya attack that took the world by storm: DIVD was in a coordinated vulnerability disclosure process with Kaseya, which was working on a patch. Some of these vulnerabilities were ultimately used in the Kaseya attack.[24]

24 https://csirt.divd.nl/2021/07/04/Kaseya-Case-Update-2/.

X OUTLOOK

As discussed above, data brokering and artificial intelligence are key focus areas of the Dutch DPA for 2020–2023. We believe the next few years will be formative for case law and legislation around data protection and AI; the knowledge on the technology has now become widely dispersed and a cohort of younger and more tech savvy lawyers and politicians is starting to weigh in on these topics. At the same time, the pace of change is reducing. This will provide a window to formalise views on these topics. Companies in this space have an opportunity to help shape the regulatory environment on these topics and would do well to make use of that, while also taking care to earn the public's trust and confidence.

We also expect more DPIAs on, and negotiations with, US large tech companies about GDPR-compliant use, similar to the above-mentioned negotiations between the Dutch government and Microsoft and Google.

Appendix 1

ABOUT THE AUTHORS

HERALD JONGEN

Greenberg Traurig LLP

Herald Jongen is an advocaat and shareholder at Greenberg Traurig LLP. Herald focuses on technology transactions, outsourcing, strategic relationships and privacy. He has led many complex multi-jurisdictional projects. He goes where the deal is, which brought him to New York, Silicon Valley, London, Paris, Brussels, Stockholm, Berlin, Frankfurt and other places. He assisted the Dutch government on the negotiations with Microsoft, which led to the landmark amendment for GDPR compliancy of Microsoft's cloud products, signed in May 2019. He also assisted the Dutch government, SURF and SIVON on the emergency negotiations with Google in the summer of 2021, to ensure continued use of Google products by schools and universities. Herald is consistently ranked in Tier 1 for IT and for Outsourcing by *Chambers* and *The Legal 500*. Quotes in these ranking guides include: 'market sources see him as a major deal maker who knows where to focus his attention'. They also highlight his up-to-the minute industry expertise, which means he is 'always in the loop with whatever's going on' and 'Herald Jongen guides the group with "supreme expertise in the field." Clients are "deeply impressed with his ability to understand the complex issues and translate them into simple concepts – an enviable strength"' and '[a]n exceptionally effective negotiator and has an excellent command of the practical issues involved with IT.'

NIENKE BERNARD

Greenberg Traurig LLP

Nienke Bernard is an advocaat and senior associate at Greenberg Traurig LLP. She has advised a wide variety of clients on data protection matters as well as on and technology-related transactions and issues, including data protection compliance, licensing and outsourcing. She also has a strong background in financial regulatory law, particularly within the context of services agreements and fintech. Nienke was Herald's wing woman on the emergency negotiations between the Dutch government, SURF and SIVON and Google in the summer of 2021, to ensure continued use of Google products by schools and universities.

EMRE YILDIRIM

Greenberg Traurig LLP

Emre Yildirim is an advocaat and senior associate at Greenberg Traurig LLP. Emre worked with clients on a wide variety of issues and transactions relating to data compliance and technology. He gained expertise in general commercial contracting and data protection compliance, in particular in the fields of regulatory matters, product development, innovative data use and outsourcing. Emre's background as a developer gives him a distinctive edge in dealing with legal matters relating to information technology.

GREENBERG TRAURIG LLP

Leidseplein 29
1017 PS Amsterdam
The Netherlands
Tel: +31 651 289 224
jongenh@gtlaw.com
bernardn@contract.gtlaw.com
yildirime@contract.gtlaw.com
www.gtlaw.com/en/Locations/Amsterdam

an LBR business

ISBN 978-1-83862-810-9