THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

© 2022 Law Business Research Ltd

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

NINTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2022
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

© 2022 Law Business Research Ltd

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADER
Katie Hodgetts

SENIOR BUSINESS DEVELOPMENT MANAGER
Rebecca Mogridge

BUSINESS DEVELOPMENT MANAGERS
Joey Kwok

BUSINESS DEVELOPMENT ASSOCIATE
Archie McEwan

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Leke Williams

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Louise Robb

SUBEDITOR
Martin Roach

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK
© 2022 Law Business Research Ltd
www.TheLawReviews.co.uk

No photocopying: copyright licences do not apply.
The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided was accurate as at September 2022, be advised that this is a developing area.
Enquiries concerning reproduction should be sent to Law Business Research, at the address above.
Enquiries concerning editorial content should be directed
to the Publisher – clare.bolton@lbresearch.com

ISBN 978-1-80449-116-4

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

© 2022 Law Business Research Ltd

ACKNOWLEDGEMENTS

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

ANDERSON LLOYD

ANJIE LAW FIRM

ASTREA

AZEVEDO SETTE ADVOGADOS

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

CHRISTOPHER & LEE ONG

CLEMENS

CTSU, SOCIEDADE DE ADVOGADOS, SP, RL, SA

GREENBERG TRAURIG LLP

KALUS KENNY INTELEX

KHODEIR AND PARTNERS

K&K ADVOCATES

KPMG CHINA

LECOCQASSOCIATE

LEE, TSAI & PARTNERS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

© 2022 Law Business Research Ltd

CONTENTS

© 2022 Law Business Research Ltd

© 2022 Law Business Research Ltd

© 2022 Law Business Research Ltd

Chapter 21

NETHERLANDS

Herald Jongen 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), the Security of Network and Information Systems Directive (the NIS Directive) and more recently the adoption of the Digital Services Act, the Digital Markets Act and the Data Governance Act. Other key upcoming European legislation include the revised NIS Directive, the ePrivacy Regulation and the Artificial Intelligence Act.

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

The past year can be characterised as anything but boring. Data protection- and security-related news was frequently the subject of press coverage and public discussion. A definite highlight was the Dutch Tax Administration being fined by the Dutch DPA for two separate major incidents: (1) its unlawful and discriminatory automated algorithmic decision making re childcare benefit applicants; and (2) its unlawful fraud blacklists. In both cases the Dutch Tax Administration was unlawfully processing the dual nationality status of citizens and discriminating them based on their dual nationality. These incidents had major repercussions for affected data subjects, including personal bankruptcy and families being torn apart due to out-of-home placement of children, and have been widely covered by the media. Following its investigation, the Dutch DPA called attention to the perils of algorithmic decision making and AI and is pushing for appropriate safeguards being in place to protect data subjects. Following the uproar caused by these incidents, the Dutch House of Representatives adopted a motion requiring mandatory human rights impact assessments for the use of algorithms intended for the evaluation of individuals or making decisions about them.[2]

1 Herald Jongen is a shareholder and Emre Yildirim is an associate at Greenberg Traurig LLP.

2 https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2022Z06024&did=2022D12329.

© 2022 Law Business Research Ltd

Enforcement by the Dutch DPA is often initiated following complaints made by data subjects, current affairs brought to public attention by politicians, or the result of investigative journalism. Data subjects continue to find their way to the Dutch DPA with complaints, but there was a decrease of almost 25 per cent in the number of complaints in 2021 compared to 2020. In its annual report for 2021, the Dutch DPA notes that it received almost 19,000 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 enforcing 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] In March 2022 the Dutch DPA published its thoughts on the upcoming European Artificial Intelligence Act, advocating for a rigorous review of high-risk AI systems.[6]

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.[7] 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 create 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 2022.

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).

3 https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2021.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 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_inzet_ai_act.pdf.

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

© 2022 Law Business Research Ltd

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 the Data Protection Officer (DPO) in an organisation.[8] In the past year we noted that 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 seemed stricter than that of other supervisory authorities and previous guidance by the Article 29 Working Party. In June 2022, correspondence between the European Commission and the Dutch DPA on this topic was leaked to the public. The European Commission disagreed and critised the Dutch DPA's position. In appeal, the Dutch DPA received a second blow on its strict views on legitimate interest by the Dutch Council of State, the highest administrative court in the Netherlands. The Council of State agreed with the lower court's dismissal of a fine imposed by the Dutch DPA but did not address whether the Dutch DPA's strict point of view is correct. We expect that the European Data Protection Board (EDPB) will publish updated guidance on legitimate interests that will clarify whether the Dutch DPA's dissenting views are justified.

iii Data subject rights

Pursuant to Chapter 3 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;

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;

8 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.

© 2022 Law Business Research Ltd

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 the Markets in Financial Instruments Regulation (MiFIR)) or via implementation of and procedures with respect to business continuity, disaster recovery and information security that are generally applicable directives such as the Capital Requirements Directive (CRD IV) and Anti Money Laundering Directive 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 the Markets in Financial Instruments Directive (MiFID)/MiFIR, requirements relating to cloud outsourcing under the European Banking Authority (EBA) guidelines and obligations to use two-factor authentication under the Payment Services Directive II (PSD II). The Financial Supervision Act mandates extensive policies to all regulated financial undertakings, including consumer credit providers and advisers and offerors of financial products.

Credit institutions, operators of trading venues (regulated markets, multilateral trading facilities (MTFs) and organised trading facilities (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.

In August 2021, the Dutch DPA approved a new Protocol for Incident Notification Systems of Financial Institutions, replacing an earlier protocol.[9] Subject to the conditions of the protocol, financial institutions may exchange data relating to fraudsters and fraudulent incidents.

9 https://autoriteitpersoonsgegevens.nl/nl/nieuws/vergunning-voor-financiele-instellingen-om-info-over-fraude-te-delen.

© 2022 Law Business Research Ltd

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 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.[10] In March 2020, the Dutch DPA published practical guidance for data subjects on the purchasing, using, selling and renting of connected cars.[11] In July 2021, the Dutch DPA published a report regarding the development of smart cities in the Netherlands.[12]

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.[13] 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 as a result of unlawful use of facial recognition.[14] 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.

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.

10 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-tips-voor-privacy-bij-internet-things-apparaten.

11 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-tips-voor-privacy-bij-connected-cars.

12 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-aanbevelingen-voor-smart-cities.

13 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-wijst-supermarkten-op-regels-gezichtsherkenning.

14 https://autoriteitpersoonsgegevens.nl/nl/nieuws/formele-waarschuwing-ap-aan-supermarkt-om-gezichtsherkenning.

© 2022 Law Business Research Ltd

In December 2019, the Dutch DPA published the outcome of an investigation into the use of tracking cookies.[15] 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.

In April 2022, the Dutch DPA updated its guidance on privacy-friendly settings of Google Analytics and noted that it has two active enforcement actions regarding the use of Google Analytics.[16] The Dutch DPA expects to be able to reach a decision on whether the use of Google Analytics is allowed in the course of 2022.

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 as well as some educational institutions commissioned data protection impact assessments (DPIAs) on Google Workspace and on the basis thereof the Ministry of Justice and Security negotiated with Google about GDPR-compliant use of Google products and services.[17] These negotiations resulted in a prior consultation of the Dutch DPA (on the basis of Article 36 Paragraph 1 GDPR). In June 2021 the Dutch DPA advised not to use Google products until the high risk identified in the DPIA were remedied.[18] The educational sector negotiated a remediation plan and an agreement on compliant use in July 2021, so that Google could still be used as of the next school year (that started in August, so that was a very close call). In May 2022, the Dutch government announced that it had

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

16 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_privacyvriendelijk_instellen_google_analytics_april_22.pdf.

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

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

© 2022 Law Business Research Ltd

reached an agreement covering the use of Google Workspace.[19] The Minister of Justice and Security expressed that the government and Google are continuing their dialogue to broaden the scope of the agreement to Google's Cloud Platform.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION AND DATA SOVEREIGNTY

The *Schrems II* judgment leads some to allege that personal data may not leave the EU at all. This is a (vocal) small minority. A slightly larger (also vocal) minority is of the opinion that personal data may not leave the EU if there is a chance, however small, that any personal data can be accessed by a foreign government outside the EU, most notably the United States. This minority rejects a risk-based approach as adopted by the Dutch Ministry of Justice and Security, as explained below. Data sovereignty is also at top of the list for Europe. And there are parties who are of the opinion that US large tech is too powerful. This mix of legal (privacy; competition law), political and economic interests and opinions leads to hefty debates, where all sides use whatever they can for the debate, often mixing up matters.

Some organisations ringfence data as much as possible within the European Union. The GAIA-X initiative was commenced to provide European organisations with a (standard for a) federated infrastructure to meet the desire for greater data sovereignty, and to be less dependent on the current offering (and terms) of hyperscalers. The GAIA-X initiative, however, had a slow start, and continues to be sluggish in its progress, seemingly in part as a result of the large and varied stakeholder landscape. And of course, it is not easy to catch up after 20 years. GAIA-X does not preclude hyperscalers from offering infrastructure as part of GAIA-X: in fact, most hyperscalers are members of GAIA-X. Hyperscalers will likely continue to play an important role in GAIA-X offerings, as they have a major head start in both infrastructure offering and the security thereof. It, however, remains to be seen whether the security of GAIA-X offerings can meet the level of security and related standards that hyperscalers offer today. That will especially be the case where hyperscalers only supply infrastructure-as-a-service (IaaS) to GAIA-X providers and play no role in the software layer and do not have access to the data and trends relevant for monitoring global threats. The French initiative Bleu (a cloud de confiance), a joint venture between Capgemini and Orange, with Microsoft as a supplier of Azure technology, but without any Microsoft involvement or access is another example.[20]

Contrary to what is stated by some who like to keep the data in the EU or to exclude US large tech, working with EU providers only to ringfence against the US CLOUD Act is not a perfect solution as the bar for not being subject to the CLOUD Act is very high. The Dutch National Cyber Security Centre (NCSC) recently published an analysis of the CLOUD Act and stated in a cover note that since European companies with data processing operations in Europe also sometimes fall under the scope of the US CLOUD Act, a thorough risk analyses is required and also realising that it is impossible to exclude extraterritorial influences completely. Therefore, 'Organisations and companies must always ask themselves

19 https://open.overheid.nl/repository/ronl-2fcdfb19e40c65ee8781dd403ee8668b6cb8a8f6/1/pdf/tk-overeenkomst-met-google-cloud-voor-google-workspace.pdf.

20 https://www.capgemini.com/news/press-releases/capgemini-and-orange-announce-plan-to-create-bleu-a-company-to-provide-a-cloud-de-confiance-in-france-2/.

© 2022 Law Business Research Ltd

against which extraterritorial legal regimes, and therefore countries, they will and can arm themselves and what that means in terms of supplier choice'.[21] In other words, choose your friends and enemies.

This fits in the Dutch government's pragmatic and positive view of the cloud, fuelled by the trailblazing landmark agreement between The Dutch State and Microsoft in 2019, and the agreement with Google in 2022. This view is also demonstrated by the risk-based assessment of data transfers, adopted by Dutch Ministry of Justice and Security in the DPIA on Teams. In February 2022, the Ministry published a DPIA on Microsoft Teams, OneDrive and SharePoint.[22] As part of this DPIA, the Ministry also published a data transfer impact assessment (DTIA), based on the Rosenthal format for DTIAs.[23] The outcome of the DTIA was, in summary, that it is extremely unlikely that personal data from Dutch government customers are unlawfully accessed by US authorities, or by authorities in other countries where Microsoft uses subprocessors. Therefore, the risk was assessed as low and the use of Teams could continue. In Austria and Germany there are some decisions that point in the direction of rejecting the risk-based approach, so it remains to be seen what the EDPB and the local supervisory authorities will say about it, if anything (soon).

The recent cloud policy of the Dutch government states that also most classified government data may be stored in the cloud, as long as certain requirements are met.

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.

Standard contractual clauses (SCC) and binding corporate rules continue to be the data transfer mechanisms that are generally most relied upon by organisations. The *Schrems II* ruling and the guidance provided by the European Data Protection Board continues to keep data controllers who use the SCC busy, while EU and US leaders are working together on yet another attempt to facilitate trans-Atlantic data transfers with a framework, this time dubbed the Trans-Atlantic Data Privacy Framework. It is yet to be seen how this framework will take shape and differ from its predecessors, and more importantly, whether it will survive the meticulous scrutiny that it will undoubtedly face.

Meanwhile, controllers are still facing the tough task to assess whether there is an adequate level of protection in the third country (the rule of law test). 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. As part of the DPIA on Teams the Dutch Ministry of Justice and Security has published an analysis of Step 3 for the United States, so this can be used by companies. The conclusion is (of course) that the US legislation does not meet the rule of law test.[24]

21 How the CLOUD-Act works in data storage in Europe | By our experts | National Cyber Security Centre (ncsc.nl).

22 https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad.

23 https://slmmicrosoftrijk.nl/wp-content/uploads/2022/02/Explanation-DTIA-on-MS-Teams-SharePoint-and-OneDrive.pdf.

24 https://slmmicrosoftrijk.nl/wp-content/uploads/2022/02/Dutch-Ministry-of-Justice-step-3-EDPB-US.pdf.

© 2022 Law Business Research Ltd

While binding corporate rules provide multinational organisations with a robust framework for international data transfers, the Dutch DPA has had a significant backlog on approving binding corporate rules for years. In its annual report of 2021, the Dutch DPA notes that it received four new binding corporate rules (BCR) requests. Owing to understaffing, the workload at the end of 2021 totalled 46 BCR requests and 27 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.

V COMPANY POLICIES AND PRACTICES

In the Netherlands, privacy policies are widely used to comply with the transparency obligations under Article 5 and Chapter 3 of the GDPR and are often published online. Most organisations have at least a basic privacy policy in place for clients and customers, 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 10 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; (2) Google Workspace; and (3) Teams OneDrive Sharepoint and Azure AD.[25]

With respect to codes of conduct under Article 40 GDPR, the Dutch DPA approved (1) the code of conduct for IT companies from the sector organisation Nederland ICT and (2) a code of conduct for processing personal data (smart meter data) by Dutch transmission network operators.[26]

25 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 and https://www.rijksoverheid.nl/documenten/publicaties/2022/02/21/public-dpia-teams-onedrive-sharepoint-and-azure-ad.

26 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/gedragscode-slim-netbeheer-goedgekeurd-door-ap#subtopic-6575.

© 2022 Law Business Research Ltd

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 recognised as such an international agreement. Transfers must also comply with other requirements regarding international transfers as described in Section IV. 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.

© 2022 Law Business Research Ltd

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 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 27 enforcement cases in 2021 and imposed a total of 11 fines.

The Dutch Tax Administration is a record holder in both the amount of fines (two) as well as the highest fine (€3.7 million) imposed by the Dutch DPA, as discussed in Section II.

In November 2021, the airline Transavia was fined €400,000 for failing to adequately secure personal data. Due to poor controls (missing access rights restrictions, easy passwords, no use of two-factor authentication), a malicious actor managed to gain access to Transavia's processing systems and obtain personal data of Transavia customers, including health data.[27]

In February 2022, DPG Media was fined €525,000 for unnecessarily requesting copies of identity documents in response to data subject requests.[28] The enforcement action was imitated following complaints of data subjects to the Dutch DPA.

In April 2022, the Dutch Ministry of Foreign Affairs was fined €565,000 for inadequately securing visa applications.[29] The Dutch DPA imposed an order (subject to penalty) to the Ministry to ensure an adequate level of security.

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.

The Collective Damages in Class Actions Act of January 2020 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. Class actions are becoming an increasingly popular instrument for interest organisations, often backed by litigation funders.

27 https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fines-transavia-poor-personal-data-security.

28 https://autoriteitpersoonsgegevens.nl/en/news/dpa-fines-dpg-media-unnecessarily-requesting-copies-identity-documents.

29 https://autoriteitpersoonsgegevens.nl/en/news/ministry-foreign-affairs-fined-inadequately-securing-visa-applications.

© 2022 Law Business Research Ltd

In last year's edition, we noted that the interest organisation Privacy Collective launched the first GDPR-related class action, 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. In December 2021 the Court of Amsterdam declared the class action to be inadmissible as it found that the Privacy Collective did not have legal standing to bring the proceedings as it failed to demonstrate it sufficiently represented the relevant data subjects. The Privacy Collective has appealed the decision of the Court. There are several ongoing class actions, including actions against Facebook and TikTok. We expect that this trend of GDPR-related class actions finding their way through the Dutch courts will continue to strengthen 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

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 Apache Log4j vulnerability discovered in December 2021 opened a massive attack vector for malicious actors: Log4j is an open-source Java logging utility that is massively used in web applications. There was a strong need to push security hotfixes to a tremendous amount of applications to prevent the vulnerability being exploited. The attack demonstrated how the various security incident response teams worked closely together to bring swift solutions.

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 2021, the Dutch DPA received about 25,000 notifications of data security breaches.[30]

Additional rules apply to government organisations and organisations in certain sectors such as healthcare and financial institutions. Mostly, requirements relating to data

30 https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2021.pdf.

© 2022 Law Business Research Ltd

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 NEderlandse Norm (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 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 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 April 2022, a bill was submitted to the House of Representatives to amend the Security of Network and Information Systems Act to ensure that certain organisations that currently fall outside of its scope, can obtain more access to threat and incident information available to the National Cyber Security Centre and mitigate any security incidents.

A key legal development has been the revised Directive on Network and Information Systems (the NIS2 Directive). The European Council and European Commission reached a provisional agreement on a draft of NIS2 on 13 May 2022 and the European Parliament is expected to vote on it in the course of 2022. The NIS2 Directive will have a significantly broader scope than the NIS Directive. The NIS2 Directive will cover all medium to large enterprises and public organisations that perform important functions for the economy or society as whole. For example, the new Directive would also cover, for instance, social media services providers and the public administration. The NIS2 Directive should also increase the level of harmonisation across member states in respect of the scope, security and incident reporting, national supervision and enforcement powers and sanctions, as well as improve pan-European collaboration of competent authorities. Though not yet in force, organisations entering into long-term agreements should consider taking stock of the requirements imposed by the NIS2 Directive to ensure future compliance.

The NCSC 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

© 2022 Law Business Research Ltd

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.

In December 2020, the European Commission launched its EU Cybersecurity Strategy for the Digital Decade. As part of this Strategy, the European Commission proposes to build, strengthen and interconnect, across the European Union security operation centres and cyber threat intelligence capabilities (monitoring, detection and analysis), with the aim to support the detection and prevention of cyber threats. One of the key envisaged actions has been the procurement of cross-border platforms for pooling data on cybersecurity threats between several member states. To that end, the European Commission has made a call for expression of interest to select organisations in member states willing to host and operate such cross-border platforms.

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.

X SOFTWARE DEVELOPMENT AND VULNERABILITIES

In April 2022, pursuant to Directive 2019/771 on certain aspects concerning contracts for the sale of goods, Dutch legislation was amended to require sellers of smart devices, software and services to continue to provide updates for as long as 'reasonably expected'.[31] A campaign was launched by the Dutch government to create awareness regarding the importance of installing the latest updates for operating systems and applications alike.[32]

The National Cyber Security Centre has adopted guidelines for the development of secure software, providing guidance for more secure development, management and provision of all forms of software.[33] The NCSC also operates a broad Coordinated Vulnerability Disclosure process.[34]

31 https://www.eerstekamer.nl/wetsvoorstel/35734_implementatiewet_richtlijnen.

32 https://veiliginternetten.nl/doejeupdates/.

33 https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beleids--en-beheersingsrichtlijnen-voor-de-ontwikkeling-van-veilige-software.

34 https://www.ncsc.nl/contact/kwetsbaarheid-melden.

© 2022 Law Business Research Ltd

XI DIGITAL GOVERNANCE AND CONVERGENCE WITH COMPETITION POLICY

In October 2021, the Dutch DPA, the Authority for the Financial Markets, the Authority for Consumers and Markets and the Commissariat for Media announced that they will collaborate more intensively to strengthen the supervision of digital activities, including technology platforms.[35]

With respect to technology transactions, the Dutch government has been implementing policies and laws aimed at reducing strategic dependence on foreign powers for vital technologies and knowledge, as well as preventing the acquisition of specific technologies, companies, infrastructure or know-how that are considered vital to the security of the Netherlands. Investment screening and approval is currently required for acquisitions in the power and telecommunications industries and a similar sectoral act is being crafted for the defence industry; a consultation on this act is expected to take place in 2023.

Additionally, a non-sector-specific piece of legislation that will apply where no sector-specific act exists was also adopted to implement the EU Foreign Direct Investment Screening Regulation. This 'Act on investment screening in respect of national security risks' will enter into force in 2023. Under this act, any transaction (broadly defined) whether initiated by a foreign or Dutch person that poses a risk to Dutch national security interests will be subject to screening and approval by the Dutch Ministry of Economic Affairs and Climate. Such a risk may be deemed to exist where the transaction could create a strategically relevant dependency of foreign powers, pose a risk to the continuity of vital processes, or impair the integrity and exclusivity of knowledge or information of vital or strategic relevance to the Netherlands. Note that in most cases control is not a requirement for a transaction to be deemed relevant (e.g., obtaining just 10 per cent of the votes in a general meeting or the ability to appoint a director may also trigger the requirement for investment screening). If the transaction is deemed to pose a risk to Dutch national security, conditions may be applied to the transaction or the transaction may be prohibited.

XII 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. Amazon Web Services (AWS) will follow shortly.

35 https://autoriteitpersoonsgegevens.nl/nl/nieuws/nederlandse-toezichthouders-versterken-toezicht-op-digitale-activiteiten-door-meer-samenwerking.

© 2022 Law Business Research Ltd

Appendix 1

ABOUT THE AUTHORS

HERALD JONGEN

Greenberg Traurig LLP

Herald Jongen is an advocaat and shareholder at Greenberg Traurig LLP. Herald focuses on tech, privacy, strategic relationship and outsourcing. He has led many complex multi-jurisdictional projects. His forte is deal-,making and 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 State on the negotiations with Microsoft HQ in Redmond, which led to the landmark agreement in 2019, and again (in 2021) on improving the commercial MS conditions for a coalition of public entities) as well as (in 2021 and 2022) on negotiations with Google. He also assisted many other Dutch and foreign public entities. Before joining Greenberg Traurig, Herald was a partner for 20 years in the corporate team of Allen & Overy, of which he was one of the founding partners. 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 note that he is '[a]n exceptionally effective negotiator and has an excellent command of the practical issues involved with IT', who 'brings a lot more to the table than legal knowledge'.

EMRE YILDIRIM

Greenberg Traurig LLP

Emre Yildirim is a 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.

© 2022 Law Business Research Ltd

GREENBERG TRAURIG LLP

Beethovenstraat 545
1083 HK Amsterdam
The Netherlands
Tel: +31 651 289 224
herald.jongen@gtlaw.com
emre.yildirim@contract.gtlaw.com
www.gtlaw.com/en/locations/amsterdam

© 2022 Law Business Research Ltd

ISBN 978-1-80449-116-4

© 2022 Law Business Research Ltd