# ANNUAL UPDATE DATA PRIVACY

2021

The General Data Protection Regulation celebrated its third anniversary in 2021. Privacy is a subject that is now on the agenda of most organisations. Moreover, the developments in this area of law are moving fast. The European and national legislators are not sitting still, and the same can be said of the supervisory authorities. Also, more and more individuals and companies seem to find their way to court when it comes to privacy. To refresh your memory, this update provides an overview of the most interesting legal developments that have taken place in this field of law in 2021 in Europe, and more specifically in the Netherlands.

## Laws and regulations

### European level

#### *International transfer*

In 2020, the privacy rules regarding international data transfers were tightened as a result of the Schrems II judgment of the Court of Justice of the European Union ('CJEU') and the subsequent guidance issued by the EDPB. In the past year a lot happened in the field of international data transfer as well. On 4 June 2021, the European Commission published new EU Standard Contractual Clauses ('SCCs') for the transfer of personal data to countries outside the European Economic Area ('EEA'). The old SCCs may no longer be used for new transfers or transfers where the underlying processing changes as of 27 September 2021. As of 27 December 2022, existing transfers can also no longer be legitimated on the basis of the old SCCs and will therefore only be allowed on the basis of the new SCCs or another legal legitimation. You can read more about the new SSCs here.

On 4 June 2021, the European Commission also published a template data processing agreement, which a controller and processor within the EEA can conclude with each other. The standard is in line with the new SSCs. Among other things, the data processing agreement includes the provision that new parties can easily accede to the agreement. The standard does not regulate liability.

#### *ePrivacy*

The negotiations about the ePrivacy Regulation ('EPV') are still proceeding and do not seem to be settled soon. The EPV relates to electronic communication and includes rules on the use of metadata, cookies and direct marketing. In February 2021, a final text proposal was adopted that has now been submitted for negotiation in the trilogue; the consultation between the European Commission, the European Parliament and the Council of Ministers. It is expected that the EPV will not enter into force before 2023 and, after a transition period of two years, will become applicable in 2025.

#### *AI Regulation*

On 21 April 2021, the European Commission presented a proposal for the Artificial Intelligence Act, also known as the AI Regulation. The AI Regulation has a risk-based approach. The more risky an AI system is, the stricter the rules that apply to it. AI systems that conflict with EU values or violate the fundamental rights and freedoms of natural persons, are even completely prohibited. The AI regulation contains a specific regime for government organisations and establishes a *European Artificial Intelligence Board*.

#### *eIDAS 2.0 Regulation*

On 3 June 2021, the European Commission presented a legislative proposal to amend the eIDAS Regulation. This proposal contains rules relating to the *European Digital Identity* and aims to improve the effectiveness of the current eIDAS regulation, extend its benefits to the private sector and facilitate reliable digital identities for all European citizens. To this end, it introduces, among others, the concept of using a *European Digital Identity Wallet*. The wallet will allow individuals to virtually store attributes, such as driving licences, diplomas and bank account numbers, and share them with organisations as they like.

### *Data Governance Act*

At the end of 2020, a legislative proposal of the Data Governance Act ('DGA') was published and on 30 November 2021 it became clear that a final text had been agreed in the trialogue. The DGA aims to facilitate and make the sharing of data from different sectors and Member States more reliable, inter alia by introducing 'data mediation services', if the data qualifies as personal data, and by contributing to the development of *European data spaces,* within which data can be freely exchanged between private and public parties, with the aim of stimulating innovation through the re-use of data. The DGA will also ensure that the possibilities for re-use of protected data from the public sector (such as personal data and data protected by intellectual property rights) are expanded. Finally, the DGA must promote the availability of data in the public interest (*data altruism*).

### *Digital Services Act & Digital Markets Act*

As we wrote in our previous privacy update, the text proposals for the Digital Services Act ('DSA') and the Digital Markets Act ('DMA') were published at the end of 2020. On 25 November 2021, the EU ministers reached an agreement on the text proposals. The DSA and DMA aim to create a safer digital space in which the fundamental rights of all users of digital services are protected and a level playing field is created to stimulate innovation, growth and competitiveness, both in the European single market and globally. The aim is to reach a final agreement in 2022. After entry into force, some of the provisions of the DSA will apply immediately and others after six months. For the DMA, the latter period is three months.

### *Data Act*

On 6 December 2021, the European Commission published the results of the public consultation on the yet to be adopted *Data Act (*'DA') that, amongst other things, will regulate access to and sharing of data between companies and public authorities in the public interest, as well as data sharing between companies. In addition, the DA will regulate the use of smart contracts in the context of data sharing, the rights to non-personal data generated in the professional use of Internet-of-Things applications, the improvement of data portability for business users of cloud services and the safeguards that should apply when non-personal data is used in an international context. Finally, the DA will amend the rules on the legal protection of databases. The European Commission's text proposal is expected in 2022.

### *Minimum digital security requirements for smart devices*

On 29 October 2021, rules were published to increase the cyber security of all wireless devices connected to the Internet. These *Internet-of-Things* devices, such as routers, security cameras, smart thermostats, refrigerators, lights and doorbells, must meet minimum requirements starting in 2024. For example, consumers must first set a strong password themselves before putting the smart device into operation, instead of a weak default password being sufficient; the smart devices must be able to be updated regularly and easily; the consumer's personal and financial data must be protected; and the consumer must be able to manage and delete the data generated.

## National level

### *Corona*

The Dutch Public Health Act ('*Wet publieke gezondheid*') was amended several times in 2021 because of the measures to prevent the spread of the Corona virus. For example, on 22 November 2021, the proposal for a Temporary Act on widening the use of corona access certificates ('*Tijdelijke wet verbreding inzet corona toegangsbewijzen')* was introduced. This legislative proposal aims to make the corona access certificate obligatory for employees in sectors where the certificate is also requested from visitors, such as the hospitality, culture and non-essential retail industry. In addition, the Dutch cabinet also wants to make it compulsory for employees to show a corona access certificate at workplaces where the risk of contamination is high. If an employer ensures a level of protection that is comparable to having a certificate, the obligation to show a corona access certificate will not apply.

### *Data Processing by Collaborative Societies Act*

The legislative proposal for a Data Processing by Cooperative Organisations Act ('*Wet gegevens-verwerking door samenwerkingsverbanden')* aims to create a legal basis for the systematic sharing and processing of personal data, including by profiling, by cooperative organisations, consisting of administrative authorities and private parties that process personal data for important public interests, such as the fight against fraud and organised crime. The proposal is currently being debated by the Dutch Senate, where it has prompted the request for further advice from the Dutch Data Protection Authority ('*Autoriteit Persoonsgegevens*'), the Council of State ('*Raad van State*') and the Institute for Human Rights ('*College voor Rechten van de Mens*'). It is not yet known when the Senate will vote on the proposal.

### Healthcare

On 3 May 2021, the proposal for an Electronic Data Interchange in Health Care Act (*'Wet elektronische gegevensuitwisseling in de zorg'*) was submitted to the Dutch House of Representatives (*'Tweede Kamer'*). Specific data exchanges will have to take place electronically. In addition, requirements may be set for language and technology, and the mandatory use of certified ICT products or services.

On 1 June 2021 the consultation version of the Care Quality Registration Act (*'Wet kwaliteitsregistraties zorg'*) was published. The legislative proposal allows, under strict conditions, to process pseudonymised personal data of patients without their consent for the purpose of quality registrations that serve a general interest and that are included in a register that the Healthcare Institute (*'Zorginstituut'*) will keep.

The Digital Government Act (*'Wet Digitale Overheid'*) lays the foundation for further digitalisation of the government and regulates, among other things, the way in which citizens and companies can log in to the government, to healthcare providers and healthcare insurers, and to pension funds. The proposal was adopted by the House of Representatives on 18 February 2020 and was amended by means of a novella following questions from the Dutch Senate (*'Eerste Kamer'*). The novella is currently being debated in the House of Representatives and, as soon as the latter has voted on it, the Senate will start it's debate on the legislative proposal and the novella.

# Supervisors

## European Data Protection Board

### *International transfer*

As previously indicated, a lot happened again in 2021 in the area of international data transfer. The EDPB recommendations 01/2020 were finally adopted on 18 June 2021. These recommendations deal with the mechanisms and measures that organisations can take to ensure that the transfer of personal data to third countries takes place in a legally valid manner. The recommendations make clear that organisations must carry out a so-called data transfer impact assessment ('DTIA') before they are allowed to transfer personal data to third countries ('non-EEA countries'). A DTIA is mandatory both when the transfer is based on SSCs and when Binding Corporate Rules ('BCRs') are used as a transfer mechanism. A DTIA is not mandatory when the transfer can be based on an adequacy decision of the European Commission. Furthermore, the EDPB discusses possible additional technical, organisational and contractual measures that can be taken if the DTIA shows that the level of protection in the third country is not sufficiently adequate. Here you can find the full roadmap of the EDPB.

An adequacy decision for the UK was adopted on 28 June 2021. With this, the European Commission indicated that the level of protection of personal data in the UK is equivalent to that in the EU. From 1 January 2021 to 28 June 2021, a transition period applied. During this period, organisations could continue to transfer personal data to the UK without the need for additional transfer mechanisms. This now remains the case. Conversely, organisations in the UK are also free to send personal data to organisations in the EU.

On 7 July 2021, guidelines on codes of conduct as a tool for transfers were published for consultation. These provide practical guidance, inter alia, on the content of codes of conduct, the process for their adoption and the actors involved, as well as the requirements and guarantees that a code of conduct for international transfers should contain.

Furthermore, guidelines on the interplay between the application of Article 3 GDPR (territorial scope of the GDPR) and the provisions on international transfers referred to in Chapter V of the GDPR were published on 18 November 2021. The guidelines are still open for consultation until 31 January 2022. As Chapter V does not define the term 'transfer', the question has arisen whether organisations in third countries that fall directly under the scope of the GDPR on the basis of Article 3, should also invoke and apply one of the transfer mechanisms listed in Chapter V when receiving personal data from organisations within the EEA. This is what these guidelines should clarify.

### *Other*

In early 2021, the EDPB published draft guidelines containing examples regarding personal data breach notification. The guidelines were finalised on 14 December 2021. These complement the previous guidelines on personal data breach notification and are intended to help organisations make decisions about the personal data breach notification and provide insight into the factors to be considered in different risk assessments.

On 2 February 2021, the EDPB published a document in response to the European Commission's request for clarification on the consistent application of the GDPR focusing on health research. In this document the EDPB announces that guidelines on the processing of personal data for scientific research purposes are being prepared. These guidelines have not yet appeared.

Furthermore, the EDPB finalised the previously published guidelines on the processing of personal data in the context of connected vehicles

and mobility related applications, virtual voice assistants, the restrictions under Article 23 GDPR and the guidelines on the targeting of social media users last year. The latter guidelines address, among other things, the responsibilities of targeters and social media providers. The main purpose of the guidelines is to clarify the division of roles and responsibilities between the social media provider and targeter.

The guidelines on the concepts of controller and processor were also finalised in 2021. The guidelines address, among other things, joint controllership and the obligations that fall directly on processors under the GDPR. The guidelines contain a number of useful flowcharts for organisations.

In October 2021, the EDPB announced that it will launch a first coordinated action targeting cloud-based services by the public sector. In such an action, the EDPB prioritises a certain topic for supervisory authorities to work on at national level. The national results will then be bundled and analysed.

On 18 November 2021, in a statement addressed to the European Commission, the EDPB expressed some concerns about the proposed Digital Services Act, Digital Markets Act, Data Governance Act and AI Regulation. In this statement, the EDPB reiterates its earlier call for a ban on the use of AI for an automated recognition of human features in publicly accessible spaces. It also urges the European Commission to consider a phase-out on the use of tracking cookies for online advertising. According to the EDPB, profiling of children should be prohibited altogether.

## Dutch Data Protection Authority

### *Budget and focus*

From 2025 onwards, the Dutch Data Protection Authority ('DPA') will have a structural budget of 8 million euros more, as follows from the Dutch coalition agreement and the corresponding budgetary annex. In the years before, the DDPA will also gradually receive a larger budget. This is in addition to the 3.6 million euros earmarked for a new algorithm supervisor that, according to the coalition agreement, will be placed with the DDPA. The budget is a lot lower than the 100 million euros that the DDPA itself had asked for.

The increased budget seems to be sorely needed, as evidenced by the extremely critical report on the DDPA by the Dutch National Ombudsman that was published just before the end of 2021. In this report, the National Ombudsman discusses the problems at the DDPA by means of two exemplary complaints from citizens, of which no fewer than 9800 were apparently on the shelf in 2020. In addition, the National Ombudsman makes a number of general recommendations to the DDPA.

In the document Focus 2020-2023: 'Data protection in a digital society', three focus areas are mentioned to which the DPA will pay extra attention in the coming years. These areas are data trade, digital government and artificial intelligence & algorithms. Thus, that focus will still be there in the coming year.

### *Enforcement*

Numerous administrative penalty decisions were published in the previous year. Not all of these penalties were imposed in 2021. Some date back to earlier years.

A fine of 440,000 euros was imposed on the OLVG, because this Dutch hospital had taken too few measures to prevent unauthorised staff from accessing medical files. The privacy rights of patients were also at stake at an orthodontic practice. A fine of 12,000 euros was imposed because patients were able to register themselves at the practice, via an unsecured website.

Although the 25 Dutch Public Health Services ('*GGD's*') did not (yet) receive a fine, the DDPA did instruct them to take more measures in the short term to better protect personal data. When, in early 2021, it appeared that data from the systems of the Dutch Public Health Services was being sold, the DDPA already intensified its supervision and started an investigation.

The Dutch Implementing body for employee insurance schemes ('UWV') was also fined for poor security. Because this organisation had not properly secured the sending of group messages via its 'My Workbook' environment, several personal data breaches occurred involving more than 15,000 people. The fine was 450,000 euros.

In addition, the DDPA fined maintenance company CP&A 15,000 euros for violations in the processing of health data of sick employees. CP&A wrongly recorded the cause of absenteeism and the absenteeism register was insufficiently secured.

Transavia received a fine of 400,000 euros in connection with poor security, which allowed a hacker to access the systems and view the personal data of 25 million people. This was not the only personal data breach that resulted in a fine within the travel sector in the Netherlands. Booking.com was also fined for reporting a personal data breach to the DDPA too late. Credit card details, among other things, were stolen during this breach. This resulted in a fine of 475,000 euros.

The PVV Overijssel (a Dutch political party) received a fine of 7,500 euros for failing to report a personal data breach to the DDPA. The breach came to light because someone had submitted a complaint to the DDPA in response to an email containing an

invitation to a meeting, in which the email addresses of all 101 recipients were visible. More information on the fines imposed on Booking.com and PVV Overijssel can be found here.

The first fine imposed by the DDPA on a Dutch government agency was a fine of 600,000 euros that was imposed on the Municipality of Enschede. The municipality was able to follow people on their phones for an extended period of time due to WiFi tracking in the city centre. An objection has been lodged against the fine.

TikTok must pay a fine of 750,000 euros. According to the DDPA, TikTok did not sufficiently explain how the app collects, processes and further uses personal data by not offering the privacy statement in the Dutch language. This constitutes a violation of the GDPR, also because the target group consists mainly of young children who are extra vulnerable.

Furthermore, Locatefamily.com was fined 525,000 euros for not appointing a representative in the EU. Organisations that fall under the scope of the GDPR are obliged to do so. Locatefamily.com is a platform where people can find contact details of family members they have lost sight of or people they would like to get in touch with. The platform contains personal data of people all over the world, including 700,000 Dutch citizens. Various European supervisory authorities received complaints about the company. Therefore, the DDPA cooperated with the Canadian and nine other European supervisory authorities in the investigation.

The fine of 2.75 million euros that was imposed on the Dutch Tax Administration is the highest fine in the Netherlands under the GDPR to date. The fine was imposed because the dual nationality of applicants for childcare benefits was processed without a legally valid basis. By unnecessarily including data on nationality, the Dutch Tax Administration was acting in a discriminatory manner as well.

### *Other*

In addition to enforcement, the DDPA also has other tasks, such as promoting public awareness and providing advice. As part of these tasks, the DDPA warned last year about the explosive increase in the number of hacks and data theft. The number of personal data breach notifications increased by no less than 30% in 2020 compared to 2019. Last year, the DDPA also launched a new reporting form for personal data breaches. You can read more about the changes to the form here.

In 2021 the DPA was critical of a number of legislative proposals, including a proposal for the Care Transparency Register Act *('Wetsvoorstel transparantieregister zorg)* and Electronic Data Interchange Act ('*Wetsvoorstel elektronische gegevensuitwisseling in de zorg*') Under the latter Act, healthcare providers would be forced to breach their medical confidentiality, because they would be obliged to exchange patient data electronically in certain situations, according to the DDPA. The DDPA was also critical of the proposed amendment to the Education Participants Register Act *('Wet register onderwijsdeelnemers')*. In addition, the DDPA called for the hiding of the home addresses of self-employed persons in the Dutch commercial register.

The DDPA also advised the Senate not to adopt the legislative proposal Data processing by cooperative ventures Act ('*Wetsvoorstel gegevensverwerking door samenwerkings-verbanden*') in its current form. The proposal gives government organisations and private parties very broad powers to share personal data with each other, for example in the event of suspicions of fraud or organised crime. According to the DDPA, the purpose of the cooperative arrangements to share, store and analyse personal data on a large scale is not described clearly enough in the proposed act. As a result, the risk of mass surveillance is lurking. Earlier, the DDPA also advised that the legislative proposal granting the Dutch National Coordinator for Counterterrorism and Security ('*Nationaal Coördinator Terrorismebestrijding en Veiligheid*') more extensive powers to collect information about citizens should be thoroughly tightened up or else not introduced at all. Both recommendations reflect the Dutch social security benefits affair and the DDPA's ongoing investigation into the Tax and Customs Administration's blacklist Fraud Detection Facility ('*Fraude Signalering Voorziening*')

Blacklists attracted the attention of the DDPA more often in 2021. For example, the DDPA rejected a licence application from the VODIOM Association for a blacklist. VODIOM wanted to share personal data of suspected fraudsters with companies in the payment, online retail and telecommunications industries. However, sharing a blacklist between companies in different sectors is only allowed in very exceptional cases and under strict conditions. This also follows from the Guide to cross-sector data sharing between private parties the DDPA published last year.

In addition to private organisations, the DDPA also addressed municipalities. The Guide Municipal Debt Assistance Act ('*Handreiking Wet gemeentelijke schuldhulpverlening*') was published containing points of attention for municipalities and professionals involved in the implementation of this Act. The DDPA also specifically addressed the recommendations for the development of so-called smart city applications to municipalities.

With the publication of the Works Council Privacy Booklet, the DDPA was aiming at a broader audience, namely employers and employees who

want to know more about the role of the works council in privacy in the workplace.

Finally, last year the DDPA published principles for the positioning of the DPO. The principles concern among other things the information position of the DPO, the resources that the DPO needs and the access of the DPO to the board of the organization. According to the DDPA, these matters are not always properly arranged within organizations.

# Case law

## European level

On 15 June 2021, the Court of Justice of the European Union ('CJEU') clarified the conditions under which national data protection authorities may exercise their powers in relation to cross-border data processing. In view of the 'One-Stop-Shop' principle, the power to take action lies, in principle, with the lead supervisory authority, although the GDPR includes exceptional situations in which the non-leading supervisory authority is nevertheless authorised to take enforcement action. This requires cooperation with the lead supervisory authority according to the established cooperation procedure and the consistency mechanism. If the non-leading supervisory authority brings an action before a national court, it does not matter whether the controller is based in another country as long as it is a Member State of the EU.

The CJEU ruled on 22 June 2021 that the Latvian registration system in which penalty points are recorded that are awarded to drivers of vehicles for road traffic offences is in breach of the GDPR. The penalty points qualify as criminal personal data and therefore fall within the scope of the GDPR. Since there are less drastic possibilities to achieve the objective of increasing road safety, the requirements of subsidiarity and necessity are not met. Moreover, the fact that this is a register accessible to the public, in which anyone can view the personal data of others without having to establish a specific interest in obtaining the data, leads to the conclusion that the registration system does not meet the requirements of the GDPR.

## National level

In 2021, 324 judgments were published on *rechtspraak.nl* (a Dutch website for national case law) in which the term GDPR occurs. We have made a selection below.

On 2 February 2021 the Court of Appeal of Amsterdam ruled that not the interim injunction procedure but the application procedure under Article 35 of the Dutch GDPR Implementation Act ('*UAVG*') is the appropriate way to achieve the removal of personal data pursuant to Article 21 GDPR. In cases in which the six-week period of Article 35 UAVG has expired, it should be borne in mind that the data subject may submit a new GDPR request, unless there is an abuse of (procedural) rights. Moreover, if the situation so requires, a preliminary injunction can be requested in an application procedure. You can read more about this application procedure in this article (available in Dutch only).

On 18 March 2021, the judge in preliminary relief proceedings in the District Court of The Hague ruled that the Dutch legislation underlying the registration of personal data of Ultimate Beneficial Owners ('UBOs') in the UBO register does not have to be declared inoperative. Although it cannot be ruled out in advance that, in the light of its objective, the public nature of the UBO register is not in line with the principle of proportionality to be observed by the European legislature, the request to refer the matter to the CJEU for a preliminary ruling will not be granted. The reason is that the *Tribunal d'arrondissement* in Luxembourg already referred questions to the CJEU on 13 November 2020. On 16 November 2021, the judgment of the judge in preliminary relief proceedings in the District Court of The Hague was upheld by the Court of Appeal of The Hague.

On 1 June 2021, the Court of Appeal of Amsterdam upheld the judgement of the District Court of Amsterdam which determined that the University of Amsterdam ('UvA') is allowed to use online proctoring software when taking exams. The use of the proctoring software is necessary for the fulfilment of the task of the UvA, due to the Covid measures. In addition, no more data are processed than necessary and in addition to that the other requirements of the GDPR are met. Moreover, the Student Council did not have the right to consent to the use of the software.

In a case about the deletion of certain parts of a care plan and additions to a final report in a file that was kept under the Youth Act ('*Jeugdwet*'), the Supreme Court ruled on 16 July 2021 that the father could not invoke the deletion scheme in the Youth Act but benefits from the additional protection under the former Dutch Personal Data Protection Act ('*Wet bescherming persoonsgegevens*' or '*Wbp*'). The Supreme Court ruled that the opinion of the Court of Appeal, that Article 11 of the Wbp assumes an objective basis for the processing of personal data and that observations of a youth care worker, which are by their nature subjective, in principle fall outside the scope of the deletion scheme, unless it can be established that these observations and observations lack any objective basis, can be upheld

because it is not incomprehensible or insufficiently substantiated by the Court of Appeal.

On 10 December 2021, the Supreme Court ruled 'for the sake of completeness' in a tax case concerning the Fraud Detection Facility ('*Fraude Signalering Voorziening*') of the Dutch Tax Administration that in exceptional situations where a tax inspection results from risk selection or on the basis of a criterion which, in relation to the taxpayer, leads to a violation of a fundamental right, such as the infringement of the prohibition on discrimination on the basis of descent, orientation or religious belief, the court may rule that the application of risk selection is so contrary to what can be expected of a properly acting public authority that the use of the results of that control must be considered inadmissible in all circumstances. In such exceptional cases, the tax inspector does not have the power to correct the taxpayer's declaration on the basis of the points revealed by the audit. According to the Supreme Court, the mere breach of the GDPR is not such an exceptional situation and cannot lead to the reduction of an, in itself correctly calculated, tax claim. If necessary, compensation for the breach of the GDPR can be claimed in separate proceedings from the general administrative court (and not from the tax court) or the civil court.

### *BKR*

After the judgments of the Court of Appeal of Den Bosch and the Court of Appeal of Arnhem-Leeuwarden on the one hand and the Court of Appeal of The Hague on the other hand, there was a lack of clarity about the legal ground on which a credit provider may process personal data in the Dutch Central Credit Information System ('*CKI*') of the Dutch Credit Registration Agency ('*BKR*'). Does the credit provider have a legal obligation or a legitimate interest within the meaning of Article 6 GDPR? The answer to the question is relevant because a data subject does not have the right to erasure and the right to objection if the data processing is based on a legal obligation. Reason enough for the judge in interim relief proceedings of the District Court of Amsterdam to ask preliminary questions to the Supreme Court, which rendered a very readable judgment on 3 December 2021.

The Supreme Court ruled that there is no legal obligation to carry out a credit registration, as the legal provisions invoked by the credit provider are insufficiently clear and precise and their application is not sufficiently predictable for those to whom the credit registration relates. However, the credit provider does have a legitimate interest in carrying out the credit registration. The person concerned by the credit registration may therefore request the erasure of data and object to the credit registration. However, even if these rights cannot be invoked because the controller has a legal obligation to process the data, the data subject is not deprived of legal protection: the processing of personal data can be challenged in the civil courts on the basis of Article 6:162 of the Dutch Civil Code (*'BW'*), whether or not in conjunction with 8 European Convention on Human Rights. Also worth mentioning is the passage in which the Supreme Court notes that the grounds for data processing in the GDPR can cumulate. This follows from the words 'at least' in Article 6 (1) GDPR. The passage is a nice addition to the judgment of the Administrative Jurisdiction Division of the Council of State ('*ABRvS*') of 22 September 2021, in which it was ruled that the assumption that personal data can never be processed if no consent has been given is not in accordance with the GDPR.

### *Compensation of damages*

In 2021, just like in 2020, many damages were claimed for violation of the GDPR. In order to obtain compensation for immaterial damage, the basic principle is that it must be proven with concrete data that damage has been suffered as a result of the violation of the GDPR. Despite the fact that this is often difficult, on 4 May 2021 the District Court of Midden-Nederland confirmed this principle in a case against the Social Security Bank ('*Sociale Verzekeringsbank*') and on 31 May 2021 the District Court of Overijssel came to the same conclusion in a case against the municipality of Almelo.

This principle - that damage must be substantiated with concrete data - does not apply if the damage is so obvious that an 'impairment of the person' can be assumed. On 12 January 2021, the District Court of Noord-Nederland ruled that 'impairment of the person' was the case because identity fraud was obvious due to the repeated publication of, among others, the national identification number of the data subject on a municipal website.

As to the amount of the damages awarded, there were two outliers in 2021. Firstly, the Court of Appeal of Arnhem-Leeuwarden that on 6 April 2021 awarded moral damages of 5,000 euros (minus 1,000 euros of moral damages that had already been awarded in the criminal case) because the appellant had been on a blacklist of the SIN Foundation ('*Stichting SIN*') for years. Secondly, on 12 July 2021, the District Court of Rotterdam awarded damages of 2,500 euros due to the nature, duration and gravity of the infringement. In this case, the municipality of Rotterdam had repeatedly refused to remove medical data from a file, had kept this medical data for too long (ten years) and had made the medical data accessible to several people and institutions.

### *Collective actions*

In 2021, several class actions were filed under the Act on the Settlement of Mass Damages Claims in Collective Actions ('*Wet afwikkeling massaschade in collectieve actie'* or '*WAMCA*'). Collective actions were initiated against TikTok on 3 June 2021, 31 August 2021 and 3 September 2021. In its decision of 13 October 2021, the District Court of Amsterdam ordered the three cases against TikTok to be held for further proceedings till 2 February 2022.

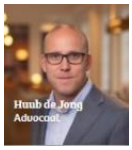
Also in 2021, there were the first verdicts in collective actions that were started in 2019 and 2020. In the case of Data Privacy Foundation ('DPS') against Facebook - which commenced before the WAMCA came into effect - the District Court of Amsterdam ruled in an interlocutory judgment on 30 June 2021 that it has jurisdiction to hear the case, that DPS is admissible because it meets the requirements of a collective action organisation, and that it is unnecessary to ask preliminary questions, as Facebook requested. The substantive hearing of the case is expected to take place this year.

On 22 September 2021, the District Court of The Hague ruled that ethnic profiling by the Royal Netherlands Marechaussee (*Koninklijke Marechaussee,* the police corps of the Dutch military) in the context of Mobile Security Monitoring (*'Mobiel Toezicht Veiligheid'* of *´MTV'*) is permitted. MTV checks are a form of foreigners' control and are aimed at combating illegal residence in the Netherlands. The Royal Netherlands Marechaussee uses ethnicity as a possible indicator when making concrete selection decisions. When determining residence status, nationality can play an important role and ethnicity can be an objective indicator of someone's supposed nationality. Since ethnicity is never the only indicator in selection decisions and these decisions must be explainable, a general ban on the use of ethnicity in MTV checks is rejected by the court. On 22 December 2021, an appeal was lodged against the ruling.

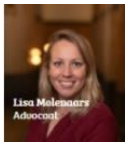
In the case of The Privacy Collective ('TPC') against Oracle and SalesForce, the District Court of Amsterdam ruled on 29 December 2021 that TPC was inadmissible because it had not been able to demonstrate that it was sufficiently representative, a requirement imposed by the WAMCA. According to the court, it cannot be determined on the basis of 75,000 *Facebook likes* whether TPC represents a sufficiently large part of the group of injured persons affected and whether the people who used the *like-button* belonged to the group of injured persons affected at all. Furthermore, TPC did not meet the requirement of being able to maintain contact with its constituency, as TPC did not register any contact details. Because of the inadmissibility, the court did not consider the merits of the case. It notes that in future cases, the question of how the GDPR and WAMCA relate to each other will therefore have to be decided.

## Want to know more?

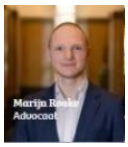
Please contact one of our privacy specialists:



Huub de Jong



Lisa Molenaars



Marijn Rooke

Esmee Fonville

Evelyn Peerboom

Tom de Wit