Five years of GDPR supervision at a glance

Ever since the General Data Protection Regulation (GDPR) came into effect, privacy has become a prominent issue. Apart from the ongoing debates on the precise interpretation of legal provisions, there have been notable developments in the enforcement actions undertaken by the Dutch Data Protection Authority. In this article, we reflect upon the fines that have been imposed by the Dutch Data Protection Authority in recent years, which have drawn significant attention. As an organization, what measures should you take to avoid being subjected to similar enforcement actions?

Laura Huijts LL.M., CIPP/E, CIPM, CIPT
is a manager at KPMG Cyber & Privacy.

Danielle Molenkamp LL.M., CIPP/E
is a consultant at KPMG Cyber & Privacy.

Malik Elbaz LL.M., CIPP/E
is a consultant at KPMG Cyber & Privacy.

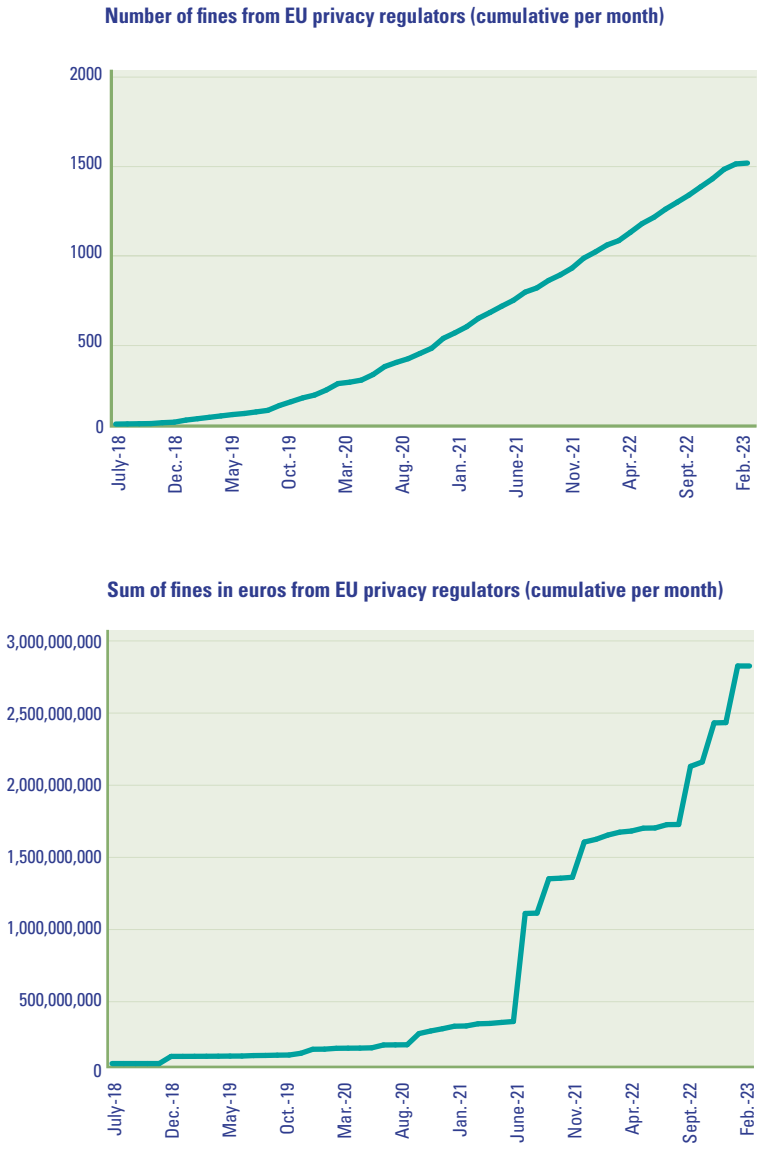
INTRODUCTION

The General Data Protection Regulation (hereinafter referred to as "GDPR") was enforced in May 2016, and organizations were granted a two-year transition period until May 2018 to align their business operations with the GDPR. After this period, the Data Protection Authorities were authorized to enforce the GDPR, including the imposition of a maximum fine of 20 million euros or 4% of an organization's annual global turnover; whichever is higher. Despite this, the Dutch Data Protection Authority (hereinafter referred to as "the Dutch DPA") has been hesitant to impose fines, even after the expiration of the transition period. Only a few fines were issued in the initial years following 2018, as per the annual reports of the Dutch DPA. The reasons cited for this were the organization's restricted capacity and the decision to allocate that capacity primarily towards significant, high-impact investigations, such as the childcare benefits scandal ("toeslagenaffaire") or issues related to the coronavirus. It was not until 2021 that the Dutch DPA began to expedite its enforcement efforts, resulting in a greater number of organizations being fined, and for larger amounts. This trend was also observed among other European Data Protection Authorities. – see Figure 1.[1]

Given the Dutch Data Protection Authority's recent implementation of regular fines, it is essential to reflect on the measures that organizations must undertake to ensure GDPR compliance and avoid facing a fine. This article examines one or more administrative fine decisions for each fine category as defined by the Dutch DPA.[2] We provide a comprehensive discussion of the following categories for which fines have been imposed by the Dutch DPA:

- inadequate basis for data processing;
- insufficient fulfilment of information obligations;
- Insufficient implementation of data subjects' rights;
- non-compliance with general data processing principles;
- inadequate technical and organizational measures;
- insufficient compliance with data breach notification requirements.

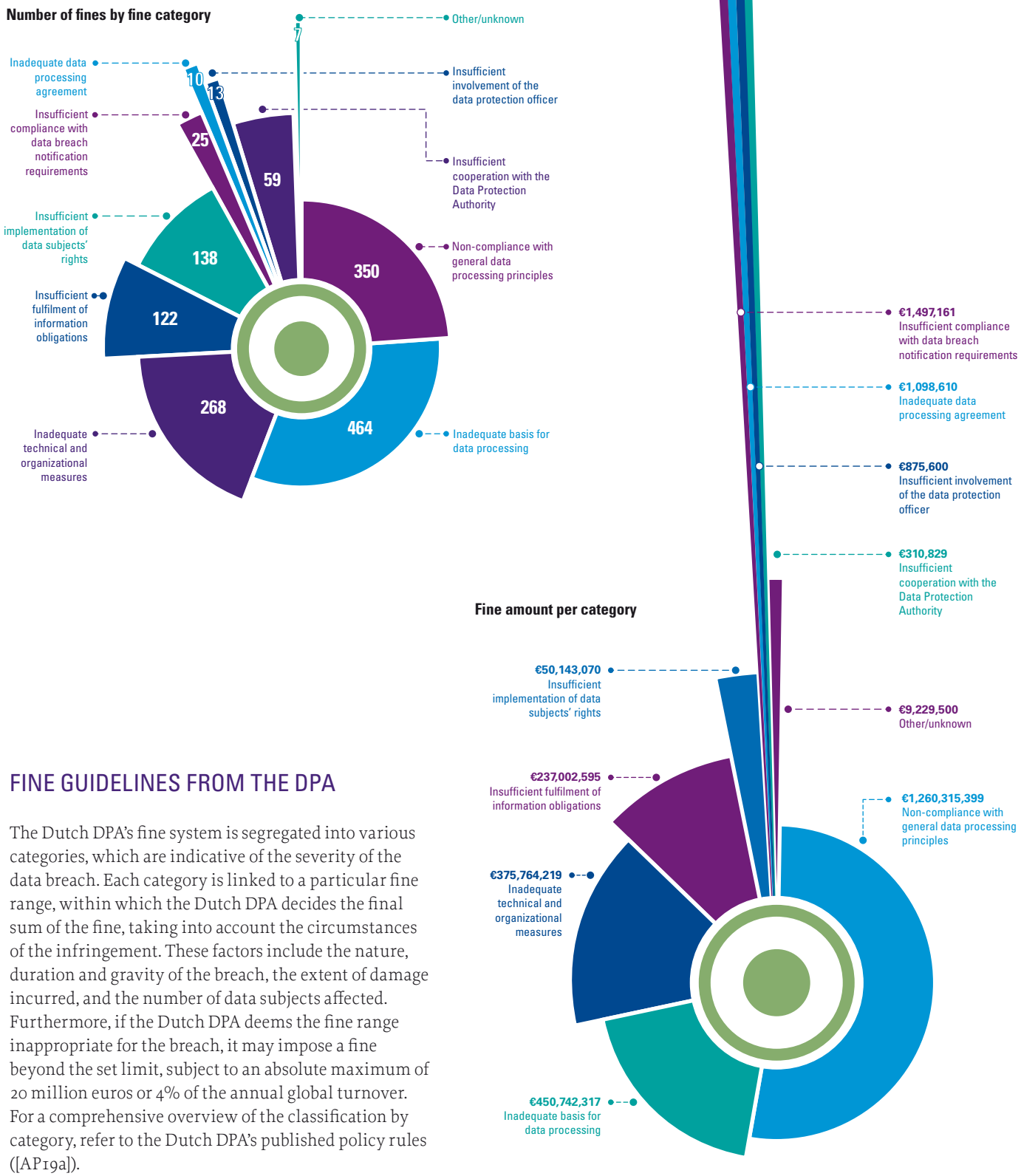
Figure 1. Overview of the number and sum of fines from European privacy regulators ([CMS23]).



1 Note that these numbers reflect only the fines disclosed and do not reflect the full number. In addition, these numbers reflect only actual fines and do not include cases where correct follow-up was given after a warning or order under fine. See also [DPA].

2 Based on the different fine categories, a selection has been made from the published fines.

Figure 2. Overview of the number and sum of fines by fine category ([CMS23]).



FINE GUIDELINES FROM THE DPA

The Dutch DPA's fine system is segregated into various categories, which are indicative of the severity of the data breach. Each category is linked to a particular fine range, within which the Dutch DPA decides the final sum of the fine, taking into account the circumstances of the infringement. These factors include the nature, duration and gravity of the breach, the extent of damage incurred, and the number of data subjects affected. Furthermore, if the Dutch DPA deems the fine range inappropriate for the breach, it may impose a fine beyond the set limit, subject to an absolute maximum of 20 million euros or 4% of the annual global turnover. For a comprehensive overview of the classification by category, refer to the Dutch DPA's published policy rules ([AP19a]).

ADMINISTRATIVE FINE DECISIONS BY THE DPA

Inadequate basis for data processing

Using fingerprints for employee time clocks based on consent

Personal data can be divided into two categories: regular and special categories of personal data. Regular personal data includes information such as name, address, and telephone number, whereas special categories of personal data comprise sensitive information such as health or political views. Due to the sensitive nature of the latter, the processing of special categories personal data is generally prohibited.

In April 2020, the Dutch DPA imposed a fine on a company for the unlawful processing of special categories of personal data ([AP19d]). The company used fingerprint scanners for employee timekeeping purposes. Fingerprints are classified as biometric data and fall under the category of special personal data. While Article 29 of the GDPR permits the processing of such data for security purposes, in this case, the fingerprints were only used for attendance and timekeeping, which does not fall under this exception. Employee consent could also be an exception, but this is generally not presumed to be freely given in a dependent relationship such as that between an employer and employee. Furthermore, obtaining consent is not enough; the company must also be able to prove it. In this case, the company was unable to prove consent, and as a result, was found to be in violation of Article 9 of the GDPR's processing prohibition. The Dutch DPA imposed a fine of €725,000.

DPA's investigation re-emphasizes the conditions imposed on the data subject's consent. Consent is legally valid when given freely, clearly and the user is sufficiently informed. It is important that refusing consent must not have any adverse consequences in any form. Consent must also be demonstrable.

WIFI tracking on a general legal basis

The processing of personal data, including regular personal data, must be based on one of the legal bases provided in Article 6 of the GDPR. The municipality of Enschede claimed that it was allowed to process personal data for the purpose of measuring crowds in the city center on the basis of performing a public task. To achieve this, eleven sensors were used to continuously capture WIFI signals from passing citizens, which were then stored under a pseudonym. However, the public task that serves as the basis for the processing of personal data must be set out in a statutory provision. The municipality relied on Article 160 of the Municipalities Act, but the Dutch DPA deemed this provision to be too broadly formulated, and stated citizens could not infer based on this article that their personal data was being processed. Moreover, the basis of legitimate interest did not apply in this situation either. As a rule, a public body cannot rely on legitimate interest as a basis, as its tasks must be defined in a statutory provision. An exception to this is when a public body acts as a private party, but this exception did not apply in this situation.

In addition to the absence of a specific legal basis for WIFI tracking, the necessity requirement was not met as measuring crowds can be done in a much less intrusive way. Furthermore, the data was stored for a long period, which could allow citizens to be tracked and patterns of living to be identified. For instance, it was possible to determine where someone worked. Due to these multiple violations, the processing by the municipality of Enschede can be considered unlawful, and the Dutch DPA imposed a fine of €600,000 ([AP21a]).

The DPA's investigation emphasizes that government organizations should be careful not to base processing operations on overly general provisions. In addition, a thorough assessment of the necessity requirement should also be made.

Using legitimate interest for purely commercial purposes

Article 6 of the GDPR mentions pursuit of a legitimate interest as the last possible basis for processing personal data. It is generally known that a public authority cannot rely on this, but there is still uncertainty as to whether a private party with exclusively commercial interests can do so.

In this regard, the Dutch tennis association "De Koninklijke Nederlandse Lawn Tennis Bond" (hereinafter referred to as KNLTB) provided personal data of its members to two sponsors for promotional purposes. One of the sponsors used members' addresses to offer discount flyers, and the other sponsor approached members by phone with an offer. The KNLTB argued that the data was provided under the guise of a legitimate interest. However, according to the Dutch DPA, their reasoning cannot be considered a legitimate interest. For a successful appeal based on a legitimate interest, the processing must be necessary to serve the interest, the interest of the data subject must not outweigh the legitimate interest, and the interest must be a legitimate interest. According to the Dutch DPA, the latter requirement means that the interest must be named as a legitimate interest in (general) legislation or elsewhere in the law. It must be an interest that is protected and enforceable in law. Moreover, the (written or unwritten) rule of law must be sufficiently clear and precise. The rule of law to which the KNLTB attached processing is freedom of enterprise. The Dutch DPA called this interest insuffi-

ciently concrete to qualify as a legitimate interest. Consequently, a fine of €525,000 was imposed on the tennis association ([AP19e]).

The KNLTB contested the fine imposed by the Dutch DPA and appealed the decision. The national court, facing uncertainties about the interpretation of the concept of "legitimate interest," referred preliminary questions to the European Court of Justice (hereinafter referred to as the ECJ). A preliminary question is a query that a national court can ask the ECJ to interpret European law. The position taken by the Dutch DPA has been previously contradicted by the European Commission and by the court in the VoetbalTV case, where the Dutch DPA took a similar stance on legitimate interest. It remains to be seen whether the Court of Justice will concur with the Dutch DPA's interpretation.

Whether a private party can process personal data based on a legitimate interest with exclusively commercial interests is not sufficiently clear from the DPA's fine decision. It is advisable to use this basis as restrictively as possible.

Insufficient fulfilment of information obligations

A privacy statement that does not match the target audience

In 2021, the widely used social media platform TikTok was fined €750,000 by the Dutch DPA for violating the requirements of the first paragraph of Article 12 of the GDPR ([AP21b]). This article stipulates that organizations must provide data subjects with information about the processing of their personal data in a concise, transparent, easily accessible, and understandable form using clear and simple language. Typically, this information is presented in the form of a privacy statement. However, TikTok's privacy statement was only available in English to its Dutch users, who primarily consist of young people under the age of 16. Given this demographic, TikTok could not assume that their users were proficient in English.

It is therefore important for organizations to determine the target audience in advance. Based on this, a comprehensible privacy statement can be drafted using an average member of the intended target group as a benchmark. It is also important that a translation of the privacy statement is available if the target group speaks a different language. If there is a target group consisting of young people, who enjoy specific protection under the GDPR, a privacy statement that is also understandable for younger target audiences will have to be drafted.

Insufficient implementation of data subjects' rights

An access request in line with Article 12 GDPR

Article 12 of the GDPR sets out specific regulations regarding the exercise of data subjects' rights, including the right to access. This right requires that the provision of data be free of charge, unless the requests made by the data subject are unfounded or excessive, particularly in cases of repetitiveness. The assessment of what constitutes repetitiveness must be done on an individual basis. The Bureau Krediet Registratie (hereinafter referred to as BKR) found this out first-hand. The BKR provided two options for submitting a right of access request: either electronically (which required payment) or once a year by post, free of charge. The Dutch DPA deemed the default requirement of electronic payment for a right of access request to be incompatible with Article 12 of the GDPR and penalized the BKR with a fine of €830,000 ([AP19c]).

According to the Dutch DPA, the option of a free annual request for access by post did not alter BKRs violation of Article 12 of the GDPR. Similarly, limiting free access to personal data to once per year via post was also found to be in violation of this provision. Whether a request for access is excessive or unfounded should be determined on a case-by-case basis, and the fact that a data subject requests access more than once per year would not necessarily make the request excessive.

Whether a request for access is excessive or unfounded should be determined on a case-by-case basis

Viewing personal data also falls under processing according to the GDPR

It is important to establish the identity of the data subject when responding to a request for access. However, DPG Media was fined by the Dutch DPA for requesting a copy of proof of identity from data subjects in order to establish their identity ([AP22a]). The DPA considered this too intrusive, especially because of the sensitive nature of identification documents. The DPA stated that the least intrusive way to identify data subjects should be used, for example by combining information already held by the controller. This could include a customer number combined with an address.

It is therefore important to ensure a free request for inspection and that, if there appears to be an excessive request, it is assessed on an individual basis. In addition, it is important for the identification process that the least intrusive means of identification is chosen. In any case, sending a copy of an identification document is considered to be too intrusive.

Non-compliance with general data processing principles

A European representative for organizations outside Europe

The GDPR applies both to organizations based in the European Union and those based outside the EU if they focus on processing personal data of EU citizens. Such was the experience of LocateFamily.com. The website did not comply with the requirement of Article 27 of the GDPR to appoint an EU representative in writing. They were under the impression that because they were not based in the EU, they did not have to comply with the GDPR. However, this was not the case and it resulted in a fine of €525,000 ([AP20d]).

Due to the international nature of the internet, organizations will more than likely process personal data of EU citizens at some point. If this is the case and your website is available in the EU, for example, and the euro can be used as currency for transactions, you will probably have to comply with the obligations of the GDPR. In that case, you also need to appoint an EU representative.

Inadequate technical and organizational measures

Inadequate security of internal systems

One of the first fines imposed by the Dutch DPA since the GDPR came into effect was against the HagaZiekenhuis. The hospital was fined because its medical patient records were not adequately secured, resulting in numerous employees accessing the files of a Dutch celebrity without any legitimate reason to do so. The hospital was obligated to monitor access, according to the Dutch DPA. Moreover, the security measures were found to be

inadequate because multi-factor authentication was not implemented. As a result of the insufficient security measures, the HagaZiekenhuis was fined €460,000 ([AP19b]).

Two years later, a similar situation occurred at another hospital, Amsterdam's OLVG. Inadequate monitoring of accessed records and insufficient security resulted in a fine of €440,000 imposed by the Dutch DPA ([AP20c]). Inadequate security of internal systems has been seen in several organizations. For example, maintenance company CP&A was fined €15,000 for inadequately securing its absence registration system ([AP20a]), the Ministry of Foreign Affairs was fined €565,000 for inadequate security of the National Visa Information System (NVIS) ([AP22b]), and the UWV had taken insufficient technical measures to secure the process for sending group messages, which resulted in a fine of €450,000 ([AP21c]).

Just like hospitals, health insurers deal with medical data of data subjects, and therefore, authorization should be established to restrict access to sensitive personal data to include only those employees who need it to perform their duties. However, the Dutch DPA conducted an investigation and found that marketing staff at health insurer Menzis had access to sensitive personal data. It is important to note that accessing personal data is also considered processing under the GDPR. Apart from inadequate access rights, Menzis also failed to maintain log files. Although there was no evidence that the marketing staff accessed this personal data, the mere possibility of such access was enough for the Dutch DPA to impose an order subject to fines for noncompliance on Menzis ([AP18]).

Viewing personal data also falls under processing according to the GDPR. It is advisable to allow only employees for whom it is necessary to have this access to this data. It is also important to ensure that systems can track who can view personal data, so that unauthorized access can be monitored.

Insufficient password requirements
In addition to multi-factor authentication, it is important to establish password requirements to prevent data breaches. In September 2019, Transavia's systems were hacked through two accounts belonging to the company's IT department. The hackers were able to access these accounts easily, as they did not require multi-factor authentication and the passwords were easily crackable, such as "12345" or "Welcome." Additionally, these accounts provided sufficient access for the hackers to breach the larger systems without further security thresholds in place. Despite Transavia's timely reporting of the data breach, the Dutch DPA imposed a fine of €400,000 ([AP21d]) due to its seriousness.

The level of security referred to in Article 32 GDPR that should be strived for depends on the risk associated with the processing. An adequate security level is determined based on various factors, such as the nature and scope of the personal data being processed.

Insufficient compliance with data breach notification requirements

Failure to report data breaches (on time)
The final category of fines pertains to the issue of data breaches, which unfortunately is a common occurrence in many organizations. Unauthorized persons may gain access to personal data, or such data may be inadvertently released or destroyed. Such an occurrence is referred to as a data leak, which must be reported to the Dutch DPA within 72 hours if there is a potential risk to the data subject(s). For instance, PVV Overijssel experienced a data leak when an email was sent to 101 recipients, making all the email addresses visible to everyone. As a result of failure to comply with the notification requirement, PVV Overijssel was fined €7,500 ([AP20b]). Booking.com was also fined for a data breach in which an unknown third party gained access to the personal data of data subjects. Because Booking.com did not report the data breach to the Dutch DPA within 72 hours of discovery, this ultimately resulted in a fine of €475,000 ([AP20e]).

Ideally, of course, you would like to prevent a data leak, for instance by taking appropriate technical and organizational measures, but this will not make it one hundred percent impermeable. In the event of a data leak, it is essential to report the data leak (in good time) in order to limit the damage for those involved and your organization as much as possible. Swift action should be taken to plug the data leak and by tightening up security, a data leak can be prevented in the future.

CONCLUSION

Although the Dutch DPA has only issued 22 public fines in recent years, this should not lead organizations to believe that they are exempt from Dutch DPA investigations and potential fines. It is a misconception that only large organizations are targeted by the Dutch DPA, as was demonstrated by the fine imposed on PVV Overijssel.

It is important to note that the Dutch DPA has significant discretion in terms of the sanctions it can impose. The range of enforcement options includes fines, orders subject to fines for noncompliance, or a combination of both. The Dutch DPA can also issue reprimands or formal warnings, although the latter appears to be used

less frequently. In fact, the last formal warning issued by the Dutch DPA was in 2020 ([AP20f]).

Organizations should strive to avoid sanctions by drawing lessons from the Dutch DPA's overview of fines. One key takeaway is the importance of having a lawful basis for processing personal data. For example, a company was fined for unlawfully processing special personal data in the form of fingerprints, while a municipality was fined for collecting location data of citizens in a disproportionate manner. The Dutch DPA has also provided guidance on the meaning of "legitimate interest" in the context of the Dutch tennis association's fining decision, although this should not be taken as the final word on the matter.

Another crucial aspect is complying with information obligations, ensuring that the target audience is taken into account. Organizations should also implement data subjects' rights effectively and employ appropriate technical and organizational measures, such as access restrictions, logging and monitoring, multi-factor authentication, and password requirements. Lastly, organizations should comply with the notification obligation towards the Dutch DPA in the event of a data breach.

It is a misconception that only large organizations are targeted by the Dutch DPA

WHAT'S NEXT?

Historically, we have seen that (published) fines were often complaint initiated. We expect this trend of the "beep system" to largely continue. It is therefore important for an organization to set up a good privacy complaints procedure, in order to resolve complaints themselves as much as possible.

The preliminary questions raised because of the fine decision on the Dutch tennis association could have major implications. Currently, the Dutch DPA differs from other Data Protection authorities, in the sense that a mere profit motive cannot be considered a legitimate interest. If confirmed by the Court, this will have major implications for all organizations that often rely on this basis.

Looking ahead, we also anticipate that the Dutch DPA will continue to pay close attention to new developments in artificial intelligence (AI), algorithms, data trading and profiling in the following years. These topics, while not as clearly reflected in the published fines, have been focal points of the DPA in recent years. Given their increasing significance in modern society and the rapid developments in these areas, we anticipate that these issues will remain a focal point for the Dutch DPA. For example, since January 2023, there is a new organizational unit within the Dutch DPA, the Algorithms Coordination Directorate, which will specifically oversee the use of algorithms.

Although the draft budget of the Ministry of Justice and Security includes a budget increase for the Dutch DPA, for instance for the establishment and work of an algorithm supervisor, the Dutch DPA mentions that its budget is insufficient to properly handle all supervisory tasks ([AP22c]). They must work with only a quarter of the budget compared to other Dutch supervisory authorities (such as the AFM or ACM, that have a budget of €100 million). We expect continued yet steady growth towards a sufficient budget over the next decade.

References

[AP] Autoriteit Persoonsgegevens (n.d.). *Boetes en andere sancties*. Retrieved from: https://www.autoriteitpersoonsgegevens.nl/nl/publicaties/boetes-en-sancties

[AP18] Autoriteit Persoonsgegevens (2018, February 15). *Last onder dwangsom en definitieve bevindingen*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_last_onder_dwangsom_menzis.pdf

[AP19a] Autoriteit Persoonsgegevens (2019, February 19). Boetebeleidsregels Autoriteit Persoonsgegevens 2019. Retrieved from: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-14586_0.pdf

[AP19b] Autoriteit Persoonsgegevens (2019, June 18). *Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf

[AP19c] Autoriteit Persoonsgegevens (2019, July 30). *Besluit tot het opleggen van een bestuurlijke boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bkr_30_juli_2019.pdf

[AP19d] Autoriteit Persoonsgegevens (2019, December 4). *Besluit tot het opleggen van een bestuurlijke boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_vingerafdrukken_personeel.pdf

[AP19e] Autoriteit Persoonsgegevens (2019, December 20). *Besluit tot het opleggen van een bestuurlijke boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_knltb.pdf

[AP20a] Autoriteit Persoonsgegevens (2020, March24). *Besluit tot het opleggen van een bestuurlijke boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_cpa_verzuimregistratie.pdf

[AP20b] Autoriteit Persoonsgegevens (2020, June 16). *Besluit tot het opleggen van een bestuurlijke boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_pvv_overijssel.pdf

[AP20c] Autoriteit Persoonsgegevens (2020, November 26). *Besluit tot het opleggen van een bestuurlijke boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_olvg.pdf

[AP20d] Autoriteit Persoonsgegevens (2020, December 10). *Besluit tot het opleggen van een bestuurlijke boete en een last onder dwangsom*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf

[AP20e] Autoriteit Persoonsgegevens (2020, December 10). *Besluit tot het opleggen van een bestuurlijke boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_booking.pdf

[AP20f] Autoriteit Persoonsgegevens (2020, December 15). *Formele waarschuwing AP aan supermarkt om gezichtsherkenning*. Retrieved from: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/formele-waarschuwing-ap-aan-supermarkt-om-gezichtsherkenning

[AP21a] Autoriteit Persoonsgegevens (2021, March 11). *Besluit tot het opleggen van een bestuurlijke boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf

[AP21b] Autoriteit Persoonsgegevens (2021, April 9). *Besluit tot het opleggen van een bestuurlijke boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_tiktok.pdf

[AP21c] Autoriteit Persoonsgegevens (2021, May 31). *Besluit tot het opleggen van een boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_uwv_beveiliging_groepsberichten.pdf

[AP21d] Autoriteit Persoonsgegevens (2021, September 23). *Besluit tot het opleggen van een boete*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_transavia.pdf

[AP22a] Autoriteit Persoonsgegevens (2022, January 14). *Besluit tot het opleggen van een boete*. Retrieved from: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_dpg.pdf

[AP22b] Autoriteit Persoonsgegevens (2022, February 24). *Besluit tot het opleggen van een boete en een last onder dwangsom*. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bz_24_februari_2022_openbare_versie_definitief.pdf

[AP22c] Autoriteit Persoonsgegevens (2022, October 24). *Informatievoorziening voor de beantwoording van feitelijke vragen door de minister voor Rechtsbescherming inzake de vaststelling van de begrotingsstaten van het Ministerie van Justitie en Veiligheid voor het jaar 2023* [Official message]. Retrieved from: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beantwoording_feitelijke_vragen_door_de_minister_voor_rechtsbescherming_inzake_vaststelling_van_de_begrotingsstaten_van_het_ministerie_van_justitie_en_veiligheid_voor_2023_-_2.pdf

[CMS23] CMS.Law (2023). *GDPR Enforcement Tracker – list of GDPR fines*. Retrieved on February 17, 2023, from: https://www.enforcementtracker.com/?insights

About the authors

Laura Huijts LL.M., CIPP/E, CIPM, CIPT is a manager at KPMG Cyber & Privacy. She has worked at KPMG since the introduction of the AVG in 2018. Laura has a legal background.

Danielle Molenkamp LL.M., CIPP/E is a consultant at KPMG Cyber & Privacy. She has a background in law and graduated from VU Amsterdam with a master's degree in Internet, IP & ICT.

Malik Elbaz LL.M., CIPP/E is a consultant at KPMG Cyber & Privacy. He recently completed a master's degree in Information Law at the University of Amsterdam.