NautaDutilh

Privacy & data in the Benelux

5 things you need to know in 2024

Intro

In 2024, we believe that as in-house counsel you will have to deal with five main developments in the area of privacy and data. By anticipating these changes, you can use them to your advantage and prepare for their impact.

#1 Privacy litigation: higher fines, corrective measures, debate on class actions and cookie control

#2 Data sovereignty: data transfers outside the EU will be subject to an increasing number of regulatory requirements

#3 Advertising tech: user consent provides the legal basis for personalised advertising

#4 EU Data Act and DGA application: a new era of data economy, open data and data sharing

#5 The notion of 'personal data': anonymisation remains difficult

In its annual plan for 2024, the Dutch Data Protection Authority (AP) has announced five central themes on which it will focus: Algorithms & Artificial Intelligence (AI), Big Tech, Freedom & Security, Data Trade and Digital Government. These themes come as no surprise, as the AP has been working on them for some time. For some of these themes, particularly the fifth, this is reflected in the published enforcement actions. AI, BigTech (with actors such as Amazon and PayPal having their EMEA headquarters in Luxembourg) and Digital Government (with the introduction of the 'Once Only Principle') are high on the agenda of Luxembourg's National Commission for Data Protection (LDPA). The Belgian DPA (BDPA) has kept its promise to work on GDPR-compliant cookies and kicked off 2024 with a landmark decision on data brokerage.

#1

↘

While the overall level of fines is expected to increase, fines are not everything. Supervisory authorities are also increasingly relying on corrective measures.

Privacy litigation: higher fines, corrective measures, debate on class actions and cookie control

The European Data Protection Board (EDPB) has updated its Guidelines 04/2022 on the calculation of administrative fines under the GDPR. It is widely expected that the overall level of fines will increase as a result. We have seen the Dutch AP become bolder, imposing a EUR 10 million fine on a sharing economy platform in January 2024, while the LDPA is still defending the EUR 746 million fine imposed on Amazon. But fines are not everything: while the BDPA's fines remain moderate, it has imposed some significant corrective measures, such as in its already landmark data brokerage case in January 2024. And in May 2023, it prohibited the transfer of personal data of Belgian 'accidental Americans' by the Belgian Federal Public Service Finance (FPS Finance) to the US tax authorities under the FATCA agreement.

Class actions in the Netherlands
The GDPR class action debate in the Netherlands will continue. A notable aspect is the discussion on whether - under article 80 GDPR - an interest group can exercise certain rights without the consent of the data subject ('opt-out'). In our view, the legislative history of Article 80 GDPR provides a strong argument for the conclusion that a collective compensation claim cannot be based on the GDPR without the consent of those concerned. This is relevant to the ongoing case in the Netherlands involving claims by interest groups against TikTok, as well as other pending claims under the Settling of Large-scale Losses or Damage Act (*Wet Afwikkeling Massaschade in Collectieve Actie* or WAMCA) for GDPR breaches.

In this context, the judgment of the District Court of Amsterdam of 25 October 2023 is relevant, where it relied exclusively on the Dutch version of Recital 142 GDPR, which states that for

collective organisations, EU member states may provide that they do not have the right to claim damages on behalf of a data subject without the data subject's authorisation. In our view, the Dutch version of Recital 142 GDPR must contain a translation error, as the EU legislator wanted to prevent a culture of litigation, which is why the right to compensation was not included in Article 80(2) GDPR. With the class action proceedings still ongoing, this will remain an important topic. You can read more about our research and opinions in our article on class actions under the GDPR.

Settlement decisions in Belgium on the use of cookies
An interesting procedural trend developing in Belgium is that of settlement decisions. The first set emerged in October and November of 2022, where the BDPA settled cases against press groups for alleged infringements related to the use of cookies on their websites through payment of EUR 10.000 per case, without imposing any further obligations under the GDPR. The cases were closed and no violation was found under the GDPR. Some have criticised these decisions, saying they give the wrong impression that organisations can avoid GDPR compliance by paying a fee.

In December 2023, the BDPA took a different approach. After five complaints filed by the NYOB against Belgian media companies for their use of cookies, it again offered settlement proposals. In these cases, the settlements were subject to the compliance with obligations instead of the payment of a sum of money. Such obligations included:

- Provide a 'Refuse all' button' next to the 'Accept all' button
- Not to make the 'Accept all' button more visually prominent than other options
- Not to make the 'Refuse all' button visually less attractive than other options
- Ensure that the procedure for withdrawing consent does not require more clicks than giving consent

These companies were given one month from the date of the settlement decision to implement the changes on their websites. In return, no infringement of the GDPR was found. We believe that this approach of the BDPA is more constructive. It will be interesting to see how this plays out in 2024.

#2

Data sovereignty: data transfers outside the EU will be subject to an increasing number of regulatory requirements

Data sovereignty in the EU, which encompasses all requirements regarding the control, access and location of data within the EU, will remain an important issue in 2024, as data transfers outside the EU will be subject to an increasing number of regulatory requirements.

↘

The EU-US Data Privacy Framework (DPF) may mark a trend that adequacy decisions adopted under the GDPR will be increasingly limited in scope, limiting their viability for international data transfers and pushing the market to offer products promising EU data sovereignty.

The EU-US Data Privacy Framework (DPF) has come into force, with only transfers of personal data to US entities that self-certify on the DPF list benefiting from the EU Commission's adequacy decision for the purposes of GDPR compliance. This may mark a trend for adequacy decisions adopted under the GDPR to have a more specific scope rather than a general recognition that a third country provides an equivalent level of data protection, as was the case with the adequacy decisions under Directive 95/46/EC which was repealed by the GDPR. The Commission also re-validated the 11 adequacy decisions adopted under the former directive on 15 January 2024, and continues to monitor the arrangements in place, in particular with the UK and the US.

Other regulatory hurdles include increased requirements for certain entities to rely on service providers located outside the EU, such as requirements for financial sector entities to have system resiliency within the EU, as well as obligations to take measures to prevent international and third country governmental access and transfer of data, such as the supplementary measures to be adopted in certain international transfers of personal data under the GDPR, and the obligations of data processing service providers in relation to non-personal data under the Data Act.

One response to the above trends has been the increased availability of products promising EU data sovereignty, such as offerings from cloud service providers that guarantee that no data will be transferred outside the EU, with the intention of avoiding regulatory hurdles and meeting the expectations that certain European customers may have. Examples include Microsoft's EU Data Boundaries programme, which went live in 2023, and the Clarence project between telecom group Proximus and Google. The Dutch government has also been quite active and successful in negotiating data sovereignty guarantees in its dealings with players such as Amazon Web Services, Microsoft and Zoom.

#3

Advertising tech: user consent provides the legal basis for personalised advertising

↘

The Digital Markets Act (DMA) marks the end of gatekeepers relying on opt-out mechanisms for the processing of their personal data for personalised advertising, requiring them to obtain the consent of end users through an opt-in mechanism.

The digital advertising sector, one of the most prominent data-driven industries, has seen a significant number of regulatory developments and high-profile cases in the recent years. This trend is set to continue in 2024. In its recitals, the Digital Markets Act (DMA) explicitly links the processing of personal data by so-called gatekeepers and the resulting barriers to competition. From 9 March 2024, the DMA requires gatekeepers to obtain the consent (opt-in) of end users for the processing of their personal data for personalised advertising, prohibiting reliance on the gatekeeper's legitimate interests. The DMA also requires that the less personalised alternative should not be different or of inferior quality compared to users who have opted in. The gatekeeper is

also bound to disclose certain data to advertisers and publishers in order to assess the performance of ads on the gatekeeper's platform.

Developments are also expected in relation to the IAB Europe's Transparency and Consent Framework (TCF). In 2022, the BDPA ruled that the original TCF did not comply with GDPR. IAB Europe appealed to the Belgian Market Court, which referred two questions to the EU Court of Justice regarding the qualification of the TC string (the digital signals created to capture data subjects' choices with respect to how personal data can be processed) as personal data and IAB Europe's role as data controller. A judgement is expected in late 2024/early 2025, which may result in changes to the TCF. A ruling on Amazon's appeal against the EUR 746 million fine imposed by the LDPA in relation to targeted advertising is also expected during 2024.

Regulators and civil society organisations are showing increasing interest in the 'pay-or-consent' mechanism used by a growing number of websites, where users who refuse to consent are asked to subscribe or pay a fee to access the website's content. On 26 January 2024, supervisory authorities in Norway, the Netherlands and Germany have asked the EDPB to issue a formal opinion on the matter, indicating that such consent may not be freely given, as required by the GDPR.

#4

↘

The Digital Governance Act and the Data Act will render data from public authorities, respectively from providers of connected products or services accessible and available, enabling easier sharing of data at the level and for the benefit of end-users, researchers and commercial entities.

EU Data Act and DGA application: a new era of data economy, open data and data sharing

The European Data Strategy aims to make the EU a leader in a data-driven society. The resulting Data Governance Act (DGA) and the Data Act have entered into force in 2023, with the first applications in member states to be expected in 2024.

The DGA is aimed at public sector bodies and sets out conditions for the re-use of certain categories of data subject to certain protections (such as personal data and intellectual property) held by said bodies, as well as rules for providing data intermediation services. It also introduces a framework to facilitate data altruism for general interest purposes. The DGA includes harmonised principles such as the prohibition of exclusive arrangements between a public sector body and a given actor, and the obligation for published non-discriminatory conditions when requesting the re-use of data. The DGA aims to complement the broader Open Data Directive, which excludes such protected data from its scope.

The Data Act applies to private and public entities, including both B2B and B2C relationships, and aims to make all data generated by the use of a connected product or service (product and service data) available to the user easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible by default.

The notion of 'personal data': anonymisation remains difficult

#5

↘

The line between anonymity and pseudonymity, and therefore when data protection frameworks such as the GDPR apply, remains unclear.

Most privacy compliance frameworks such as the GDPR do not protect anonymised data, as it can no longer lead to an identified or identifiable person. However, these frameworks do apply to pseudonymised data when such data can still lead to an identified or identifiable person with additional information. The line between anonymity and pseudonymity, and therefore when such privacy frameworks apply, remains however unclear.

There is some debate as to whether the SRB case (before the EU General Court, currently under appeal before the CJEU) concluded on a new risk-based approach to define anonymisation from the perspective of the recipient of such data. In our view, this was already the conclusion reached in the Breyer case and the 2023 Scania case before the CJEU. If a data recipient does not have additional information to re-identify the data subjects and/or does not have legal means to access such information, the transferred data can be considered anonymised. However, the SRB case highlights that a supervisory authority must assess whether data is anonymised or not from the perspective of the recipient, and cannot assume by default that there is no anonymisation and expect the parties to prove otherwise.

The issue of anonymisation remains key, not only in data sharing initiatives at the European level such as the Data Governance Act and the European Health Data Space. It is fundamental in data-driven industries and, in particular, in the development of AI products. Aggregated data relied upon in such cases may still be considered personal data and subject to the above privacy frameworks (and their limits on international transfers). However, it should be examined if there are means to de-identify the data.

About the team

NautaDutilh's Technology & Privacy team combines in-depth knowledge and understanding of its clients, their technologies and sectors with a pragmatic approach to solving legal issues. The team operates at the intersection of technological innovation and the law, focusing on finding creative solutions to technology-driven challenges. Our team members are skilled in advising on fast-growing and emerging new technologies, including cloud computing, cybersecurity, data monetisation, open source software, AI, OTT, fintech and distributed ledger technology. In addition, the team has extensive experience in advising clients on a wide range of data protection issues. This includes conducting GDPR gap analyses, drafting and reviewing privacy policies, advising on international data transfers, data protection provisions in contracts and employee monitoring, and liaising with data protection authorities.

Contact

For further information on these developments and their implications, please contact:

Joris Willems The Netherlands
T: +31 6 5 20 50 390
joris.willems@nautadutilh.com

Vincent Wellens Luxembourg/ Belgium
T: +352 621 15 61 78
vincent.wellens@nautadutilh.com

Contributors

Anke Holtland | Terrence Dom | Sarah Zadeh | Danique Knibbeler | Matthieu Pierre | Garance Diacono | Jill Van Overbeke | Aline Bleicher | Ottavio Covolo | Sophie Denissen | Inger van Dijkman