NautaDutilh

Benelux Data Law

things you need to know in 2023

Intro

In 2023, we believe that you, as in-house counsel, will have to deal with five main developments in the area of data in the Benelux. By anticipating these changes, you can use them to your advantage and prepare for their impact. The five main developments we have identified are:

#1 New EU-US data privacy framework & international data transfers

#2 Procedural evolutions: settlements and class actions

#3 Higher fines

#4 Update on European data strategy: the open data movement

#5 E-archiving harmonisation and the eID wallet

#1

↘

The EU-US DPF will allow data to flow freely between the EU and US companies certified under the new framework.

New EU-US data privacy framework & international data transfers

In July 2020 the European Court of Justice invalidated the Privacy Shield which was a basis for legitimate transfers of personal data from the EU to self-certified commercial organisations (for example, in the context of intra-group transfers and/or in the course of deployment of cloud services provided by US groups). For more than two years, this left EU data controllers without a general legal framework to enable EU-US personal data transfers. It caused an increased burden of organising data transfer impact assessments ("DTIAs"), organising adequacy otherwise than via the signature of standard contractual clauses ("SCCs") and, in nearly all cases, supplementary measures to avoid US government access.

However, a new framework under the name "EU-US Data Privacy Framework" ("EU-US DPF") is expected to be finally adopted this spring. On 7 October 2022 President Biden signed an Executive Order setting out the measures the U.S. will take to implement its commitments under the EU-US data privacy framework ("Biden EO") announced by President Biden and European Commission President von der Leyen in March 2022. Such measures are targeted at reducing the risk of unjustifiable government data access and improving the means of judicial redress in this context. Once adopted, the EU-US DPF will allow personal data to flow freely between the EU and US companies certified under the new EU-US DPF. US companies will be able to join the framework by committing to comply with a detailed set of privacy obligations that are yet to be released by the US Department of Commerce. On 13 December 2022, in any event, the European Commission published its draft adequacy decision in relation to the EU-US DPF, which should give interested US companies a good grasp of what will be expected in order to be self-certified.

Although not yet final, we recommend already taking the Biden EO into account by means of the following three actions:

- Update your EU-US DTIAs to reflect the reduced risk of unjustifiable government data access following the Biden EO. Such updates may lead to a reduced need for supplementary measures.

- Check whether your most important US suppliers and personal data recipients plan to obtain certification by the US Department of Commerce under the new EU-US data privacy framework. If not, ensure that (1) the most recent set of the standard contractual clauses (version June 2021; implementation deadline was 27 December 2022) are in place, (2) the DTIA is up to date and (3) any supplementary measures (if still required) are implemented.

- Monitor the next adoption steps and, in particular, the position of the EDPB, which has to give its opinion of the draft EU-US DPF adequacy decision in the coming months, and of the DPA(s) that have jurisdiction. To date, the Benelux DPAs have not taken a position in relation to the Biden EO, but the Data Protection Authority of the German state of Baden-Wuerttemberg has voiced criticisms that are similar to those of NYOB, the non-profit organisation led by Max Schrems.

On a more general note, do not forget that multiple processing activities entail transfers to other non-EU/EEA countries besides the US and that the specific GDPR provisions on international data transfers must also be complied with for transfers to those countries as well.

#2

Procedural evolutions: settlements and class actions

In 2022 some interesting procedural evolutions were announced in the Benelux, which will be sure to materialise and further evolve in 2023.

↘

Procedural evolutions related to settlements and class actions will materialise and further evolve in 2023.

In late October 2022, the Belgian Data Protection Authority issued two settlement decisions against data controllers for alleged cookie infringements through payments of 10,000 EUR per case. The settlement proposals were made after the proceedings before the Litigation Chamber had already begun, which seems to be a first in the EU. This procedural evolution is thus a very interesting avenue for data controllers to explore when confronted with proceedings before the Belgian Data Protection Authority, especially since the settlement amounts are significantly lower than the penalty amounts in comparable cases. The Luxembourg DPA also has an interesting scheme to settle complaints at an early stage of the procedure, but such settlement will not take place before the official opening of a sanction procedure. We predict that other data protection authorities will explore this procedural avenue as well in order to deal with the continuous rise of data protection complaints.

2022 saw the rise of class actions in the Netherlands against multinational big tech companies, in line with the increased recognition at EU level of avenues to bring class actions for data protection infringements (i.e. the Meta case in which the CJEU ruled that consumer protections associations may bring representative actions against personal data protection infringements). The Netherlands is popular for class actions in Europe. An interesting ongoing class action case in the Netherlands concerns the claim from the Take Back Your Privacy Foundation (TBYP) against TikTok. TBYP has filed the class action under the Dutch Act on Mass Damages Settlement in Class Actions (Wet Afwikkeling Massaschade in Collectieve Actie or WAMCA). WAMCA provides

for an opt-out regime, meaning that even injured parties that did not actively sign up for the claim are bound by the judgement unless they actively opt-out. TBYP claims that TikTok infringes the GDPR on multiple grounds, regarding lawfulness, transparency, international data transfers and data security, in relation to the personal data of children. TBYP has demanded that TikTok pays substantial damages to all children and stops its unlawful actions. TikTok has argued that the Dutch court did not have jurisdiction to adjudicate the case because the company was based outside the Netherlands. The Dutch court ruled that this was incorrect and that it had jurisdiction to rule on these claims. The decision will allow the proceedings to continue. If TBYP wins, it will be the first successful privacy class action in the Netherlands. This means that especially companies that process large volumes of personal data should anticipate potential privacy class actions.

#3

Higher fines

↘

The EDPB's Guidelines are expected to further accelerate the trend of supervising authorities to impose higher penalties against larger organisations.

Last year the European Data Protection Board ("EDPB") issued the Guidelines 04/2022 on the calculation of administrative fines under the GDPR. The Guidelines are intended for use by the supervisory authorities and seek to establish harmonised "starting points" for the calculation of a fine by means of a detailed five-step methodology. Thereby, the EDPB also clarifies how to determine the turnover of an undertaking, given that fines under the GDPR can be up to 4% of the worldwide turnover of the preceding financial year. The Guidelines reconfirm the discretionary power of supervising authorities to apply the full range of fines, from the minimum amount up to the legal maximum set out in the GDPR, and that they are even allowed to use predetermined fixed amount fines for certain infringements. Overall and taking into account the EDPB's harmonised "starting points", these Guidelines are expected to further accelerate the trend of supervising authorities to impose higher penalties against larger organisations, as the Luxembourg Data Protection Authority did by fining Amazon for a record amount of EUR 746 million and the Dutch Data Protection Authority by imposing a fine of 3.7 million on the Dutch Tax Administration.

#4

Update on European data strategy: the open data movement

The European data strategy that was announced by the European Commission in 2020 aims to create a single market for data, in which data will flow freely across sectors benefiting various stakeholders, boosting Europe's global competitiveness and data sovereignty. The European Commission published the Data Governance Act (DGA) and the Data Act (DA) as legislative initiatives in connection with this strategy. 'Data' in this context should be interpreted broadly and includes both personal data and non-personal data. The DA is still in the proposal phase, while the DGA will apply from

↘

The European data strategy and the related legislative proposals show that the open data movement is a priority of the European Commission.

24 September 2023. The DGA includes conditions for the re-use of certain categories of data held by public sector bodies, sets rules for the provision of data intermediation services, and introduces a framework that facilitates data altruism for objectives of general interest. Entities that already provided data intermediation services on 23 June 2022 have an extended deadline – 24 September 2025 – to ensure compliance with the specific provisions in the DGA on data intermediation services. The DA aims to ensure fairness in the digital environment, stimulate a competitive data market, open opportunities for data-driven innovation and make data more accessible for all. It includes harmonised rules on (i) making data generated by the use of a product or related service available to the user of that product or service, (ii) making data available by data holders to data recipients, public sector bodies and Union institutions, agencies or bodies, (iii) facilitating switching between data processing services, (iv) introducing safeguards against unlawful third party access to non-personal data, and (v) the development of interoperability standards for data to be accessed, transferred and used. The European data strategy and the related legislative proposals show that the open data movement is a priority of the European Commission. On the one hand, these initiatives should increase the movement of open data, leading to benefits such as data-driven innovations and a competitive data market. On the other, these initiatives introduce obligations for non-personal data similar to those under the GDPR. Personal data remain subject to the General Data Protection Regulation (GDPR).

#5

E-archiving harmonisation and the eID wallet

↘

The updated eIDAS Regulation is expected to be adopted in 2023.

The 2014 eIDAS Regulation (EU) introduced common rules on e-identification and e-signatures, and furthermore introduced several other so-called “trust services”, such as the electronic seal and time stamp. The eIDAS Regulation, however, falls short in a twofold way: (1) the eID part of the eIDAS Regulation is inherently limited to the public sector, and furthermore only led to 14 Member States giving notification of at least one eID scheme; and (2) the Regulation fails to harmonise the rules on e-archiving. To remedy such shortcomings and more generally increase cross-border reliance, a proposal to update the eIDAS Regulation was published in mid-June 2021 which:

- Creates a European Digital Identity Wallet that allows users to store identity data, credentials and attributes linked to their identity and to the extent necessary to use these for purposes of interaction with both public sector and private sector players (e.g. for authentication (online and offline) for a service; to sign via qualified electronic signature, etc.).

- Now obliges Member States to notify of at least one Electronic Identification Scheme which can be used both online and offline.

- Introduces three new qualified trust services: qualified electronic archiving services, electronic ledgers and the management of remote qualified signature and seal creation devices. The qualified electronic archiving service legal framework will facilitate cross border recognition of qualified electronic archiving services and thus remedy the uncertainty resulting from the different sets of Member State requirement regarding e-archiving.

The creation of the European Digital Identity Wallet is the topic that is currently slowing down the legislative process, given that it raises a number of data protection concerns regrouped around the fact that such a European Digital Identity Wallet stores a large number of personal data, including sensitive personal data, which would be used for a large variety of use cases across different sectors and Member States. This obviously entails an important risk of identity theft and data oversharing. Once a compromise is reached on this topic, we expect the further adoption process to go quickly, so that the updated eIDAS Regulation may well be adopted in 2023.

About the team

NautaDutilh's Technology & Data Protection Team combines in-depth knowledge and understanding of its clients, their technologies and sectors with a pragmatic approach to resolving legal issues. The team is active at the intersection of technological innovation and the law and focuses on finding creative solutions to technology-driven challenges. Our team members are skilled at advising on fast-growing and emerging new technologies, including cloud computing, cybersecurity, data monetisation, open-source software, AI, OTT, Fintech and distributed ledger technology. The team further has extensive experience in advising clients on the widest range of data protection issues. These include conducting GDPR gap analyses, the drafting and review of privacy statements, advising on international transfers of data, data protection provisions in contracts and employee monitoring, as well as liaising with data protection authorities. The team is regularly praised for its dedication to clients, rapid response time and practical, high-quality advice.

Contact

For more information, please contact

Joris Willems Netherlands
+31 20 71 71 670
+31 6 52 05 03 90
Joris.Willems@nautadutilh.com

Vincent Wellens Luxembourg / Belgium
+352 26 12 29 34
+352 621 15 61 78
Vincent.Wellens@nautadutilh.com

Contributors

Terrence Dom | Danique Knibbeler | Carmen Schellekens | Sarah Zadeh