GDPR Update October 2018 - Overview of developments since May 25 2018

October 4, 2018

Recent developments in the European Union (EU)

Article 29 Working Party replaced by the European Data Protection Board

As of May 25, 2018 the Article 29 Working Party ceased to exist and has been replaced by the European Data Protection Board (the EDPB). The EDPB is an independent EU decision-making-body with legal personality that contributes to the consistent application of data protection rules throughout the EU and promotes (cross-border) cooperation between supervisory authorities. The EDPB is established by the GDPR and is composed of the heads of the supervisory authorities of each EU Member State and of the European Data Protection Supervisor (the EDPS), or their representatives. The EDPB is empowered to take legally binding decisions e.g. in case supervisory authorities have conflicting views regarding competence. EDPB's tasks are listed in Clause 70 GDPR.

EDPB publications and EDPB statement on the ePrivacy Regulation

During the first plenary meeting on May 25, 2018, the EDPB has adopted a draft version of the Guidelines on certification. Public consultation for this guideline was available until July 12, 2018. The EDPB has also adopted the final version of the Guidelines on derogations applicable to international transfers (article 49).

In addition to the above, the EDPB has adopted a statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications.

Resolution on the adequacy of the protection afforded by the EU-US Privacy Shield

The EU-US Privacy Shield is an agreement between the EU and the US, allowing for transatlantic exchanges of personal data between EU and US companies. When a US company is certified under the EU-US Privacy Shield, the company is considered to be established in a third country that is deemed to have an adequate level of data protection. Consequently, a transfer of personal data from EU to such company in the US is allowed.

In July 2018, the European Parliament adopted a resolution in which it takes the view that the Privacy Shield arrangement does not provide the required level of protection as required by Union data protection law and the EU Charter. In the resolution the members of the European Parliament have called for suspension of the EU-US Privacy Shield, unless the US authorities fully comply with its terms by September 1, 2018.

So far, the EU-US Privacy Shield is still in place, but we continue to recommend that our clients be careful to rely solely on the EU-US Privacy Shield as a means to transferring personal data from the EU to the US.

Administrator of Facebook fan page jointly responsible with Facebook

The Court of Justice of the European Union (the Court) ruled that a fan page administrator on Facebook is jointly

responsible with Facebook for the processing of personal data of fan page visitors through the use of Facebook Insights. In the present case, the administrator of the fan page is a German organisation, *Wirtschaftsakademie Schleswig-Holstein*, which operates in the field of education and offers educational services inter alia by means of a fan page hosted on Facebook.

The Court reasoned that *Wirtschaftsakademie* made it possible for Facebook to collect personal data of fan page visitors by creating the fan page (Facebook is enabled to place cookies on the device of the fan page visitor). In that context, *Wirtschaftsakademie* was also able (with the help of filters made available by Facebook) to define the criteria in accordance with which statistics for advertising purposes were to be drawn up by Facebook. The fan page administrator even has the possibility to designate the categories of persons whose personal data is to be made use of by Facebook. In this way the fan page administrator assists Facebook in the processing of personal data via its fan page and should therefore be regarded a joint controller. Importantly, the court states very clearly that joint responsibility does not require that each of the controllers has access to the personal data concerned.

The Court's decision is based on the Directive (as repealed from May 25, 2018). However, as under the GDPR the concept of "data controller" remains unchanged, this Court's ruling is of relevance under the current legal framework as well.

In response to the Court ruling, Facebook prepared a joint controller addendum that any user of Facebook Insights is now required to accept.

Complaints against Google, Facebook, Instagram and WhatsApp by privacy group noyb.eu

On the first day after the GDPR became applicable, privacy group Noyb.eu (led by privacy activist Max Schrems) filed (pdf) four complaints about "forced consent" with four different supervisory authorities (i.e. the supervisory authorities of France, Belgium, Hamburg and Austria) against Google, Facebook, Instagram and WhatsApp. To date, further updates about the consequences / follow up of the complaints by the supervisory authorities have not been announced.

CNIL serves formal notice to two advertising start-ups to obtain user's consent for processing geolocation data for ad targeting

The French Data Protection Authority (CNIL) has given formal notices (French only) to two advertising start-ups in France, i.e. FIDZUP and TEEMO.

FIDZUP, a company having partnerships with various mobile application publishers, developed a tracking tool that was implemented in the applications of the mobile application publishers. In this way, FIDZUP was able to collect MAC addresses and mobile advertising IDs from application users. Further, FIDZUP placed Wi-Fi routers in different retail stores, registering MAC addresses of individuals within the router's range. FIDZUP combined the collected data and consequently was able to make a link between the MAC addresses collected via the application and the MAC addresses collected via the Wi-Fi routers. This enabled FIDZUP to show users advertisements on their smartphones based on their location.

According to CNIL, FIDZUP did not obtain users' consent in accordance with the GDPR. When installing the app, users were requested to give their consent on the collection of geographical data. CNIL considered this consent not to be "informed". Users were for example not informed about the advertising purposes and the identity of FIDZUP. This information was only provided to the users after the collection of personal data by FIDZUP (which should have been available to the user prior to the collection of personal data). Furthermore, CNIL considered the consent not to be "freely given", as it was not possible for individuals to download the app without the tracking tool.

According to CNIL, the information with regard to the Wi-Fi routers collecting personal data was also provided too late. Individuals were informed of the personal data processing through hardcopy posters in the stores. However, once the individuals could actually notice the posters, their personal data had already been collected.

TEEMO is similar to FIDZUP. Also TEEMO was able to collect information about the geographical location of application users, via a tracking tool. With the information, TEEMO was able to build profiles of these users and target them with advertising based on these profiles.

According to CNIL, TEEMO had not obtained users' consent in accordance with the GDPR. Firstly, because at the moment of the installation of the application, users were not informed about the fact that their geographical location data would be collected for profiling purposes. This information was only provided after installation (at which moment, the personal data had been collected already). Secondly, it was not possible for users to download the applications without the tracking tool. This means that consent was not freely given.

Both companies are ordered by the CNIL to obtain users' valid consent within three months. If they fail to do so, the CNIL will likely issue further sanctions.

Recent developments in the Netherlands

More than 600 complaints lodged with the DDPA

More than 600 individuals have already filed a privacy complaint (Dutch only) with the Dutch Data Protection Authority (the DDPA; *Autoriteit Persoonsgegevens*). On June 29, 2018, the DDPA had already analyzed the first 400 complaints. Almost a third of the complaints relates to problems with erasure requests. Other complaints mostly concern unwanted disclosure of data to third parties (18 percent) and issues with access requests (5 percent).

Supervisory framework of the DDPA

On May 25, 2018, the AP published its supervisory framework (pdf; Dutch only). The DDPA initially focuses on compliance with the accountability of organizations through research and by commissioning organizations to provide relevant information.

In this context, the DDPA investigated whether the organizations obliged to appoint a Data Protection Officer (a DPO), have actually done so. The DDPA focused on governments and healthcare institutions. For more than 400 government organizations the DDPA verified whether they had appointed a DPO and registered him/her with the DDPA. The initial results showed that less than four percent of the organizations had not (yet) appointed a DPO. After being contacted by the DDPA, these organizations were given a remedy period until June 11, 2018. On September 3, 2018, the AP announced (Dutch only) that only one of the investigated organisations remained that had not yet appointed a DPO, but it would do so shortly.

According to DDPA's supervisory framework, other focus areas are the processing of medical data, the trade in personal data and data breaches, in particular unreported data breaches and those (at least in part) resulting from serious shortcomings in data security.

On July 17, 2018, the DDPA announced (Dutch only) an investigation into large private companies on compliance with the GDPR. Thirty large private companies in ten different private sectors were subject to DDPA investigations into the implementation of the mandatory register of processing activities. The DDPA takes the view that having a complete and accurate record of processing activities in place, is an indication that the organization is taking its data protection obligations seriously.

On September 17, DDPA's chair announced in a radio interview that several companies have received penalties which

become payable if they do not comply with the GDPR at a date set by the DDPA. The DDPA has not made public which companies it concerns or which GDPR breaches it regards, and how long the remedy period is. It does seem to confirm that the DDPA continues its pre-GDPR practice of not immediately issuing a fine in case of breach, but first allowing organizations a remedy period. However, the DDPA's chair also made clear that if organizations deliberately breach the GDPR, the DDPA will issue fines immediately.

Adaptation of national legislation to the GDPR (*Aanpassingswet Algemene Verordening Gegevensbescherming*)

As a result of the GDPR (which has direct effect in Dutch law) and the Dutch GDPR Implementation Act, it is necessary to amend various national laws that still contain references to the Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*) or where obsolete terminology is still being used. The relevant Act (*Aanpassingswet AVG/UAVG; Dutch only*) has entered into force (Dutch only) and has retroactive effect to May 25, 2018, the date on which the GDPR became applicable.

Dutch Tax Authorities process citizen service number in violation with the GDPR

The DDPA has concluded (Dutch only) that the Dutch Tax Authorities have no legal basis to use the citizen service number (BSN) in the VAT identification number of self-employed persons with sole proprietorship. According to the DDPA, processing citizen service numbers also violates article 5(1)(a) and article 6(1) GDPR (i.e. the principles of lawfulness, fairness and transparency, and the legal bases for processing respectively.)

In the Netherlands self-employed persons with a sole proprietorship that are subject to the VAT legislation, are obliged to register for a VAT number at the Dutch Tax Authorities. The VAT Number mainly consists of such person's citizen service number (*Burgerservicenummer;* BSN). The BSN is a unique number for everyone who has dealings with the Dutch government. It is being used to facilitate communication between the government and citizens.

VAT numbers must be included on invoices and the website of these self-employed persons, which means that everyone is able to deduct the BSN of these self-employed persons. This could lead to identity fraud or other forms of misuse.

Article 87 GDPR gives member states the right to set their own conditions for processing national identification numbers. This is implemented in article 46 Dutch GDPR Implementation Act. Processing the BSN is only lawful if there is a law that explicitly states that the BSN may be processed and used for a specific purpose. This is not the case for VAT numbers.

The Dutch Tax Authorities must refrain from processing the citizen service numbers before January 1, 2019. However, it has already become clear (Dutch only) that the Dutch Tax Authorities will not be able to adjust their systems before that date.

Dutch national police penalized for failing to monitor access / use personal data

In 2015 the DDPA conducted a research after the use of personal data by the Dutch national police in the computer system that is used to monitor incoming and outgoing individuals and goods in the Schengen Area. In that research, the DDPA found several vulnerabilities in the system. One of those was that the Dutch national police did not (carefully) monitor the log files with information about who accessed certain data with enough scrutiny. The DDPA stressed that monitoring logging details is an important tool for checking if personal data is accessed or used unauthorized. The national police did not solve this problem within the time frame set by the DDPA and was therefore fined € 40,000. Although this decision dates back to the Directive, it is still relevant.

Warning against misleading GDPR certification

Through a recent press release, the DDPA warns organizations against misleading GDPR certifications. There are companies that assert they can issue GDPR certifications that will allow organizations to demonstrate compliance with the GDPR. These companies pretend to work closely with the DDPA on privacy legislation, which is not the case. Only certification bodies that have been approved (accredited) by the Dutch Accreditation Council (Raad van Accreditatie) would be allowed to issue such GDPR certifications. However, to date, no certification bodies have been accredited.

Please click here to subscribe to our monthly updates on the GDPR.

Overview of subjects

January 2017	Territorial scope of the GDPR (Dutch)
February 2017	The Concept of Consent
March 2017	Sensitive Data
April 2017	Accountability, Privacy by Design and Privacy by Default
May 2017	Rights of Data Subjects (information notices)
June 2017	Rights of Data Subjects (access, rectification and portability)
July2017	Rights of Data Subjects (erasure, restriction, objectand automated individual decision-making)
August 2017	Data Processors
September 2017	Data Breaches and Notifications
October 2017	Data Protection Officers
November 2017	Transfer of Personal Data (outside the EEA)
December 2017	Regulators (competence, tasks and powers)
January 2018	One Stop Shop
February 2018	Sanctions
March 2018	Processing of Personal Data in the Employment Context
April 2018	Profiling and Retail
May 2018	Overview
October 2018	Overview of developments since May 25, 2018

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08
marc.elshof@dentons.com

Celine van Es
Associate, Amsterdam
D +31 20 795 31 22
M +31 6 11 16 30 45
celine.vanes@dentons.com