SIGN UP

PANGEANET

INTERNATIONAL NETWORK OF INDEPENDANT LAW FIRMS

VISIT OUR WEBSITE

NEWSLETTER 3

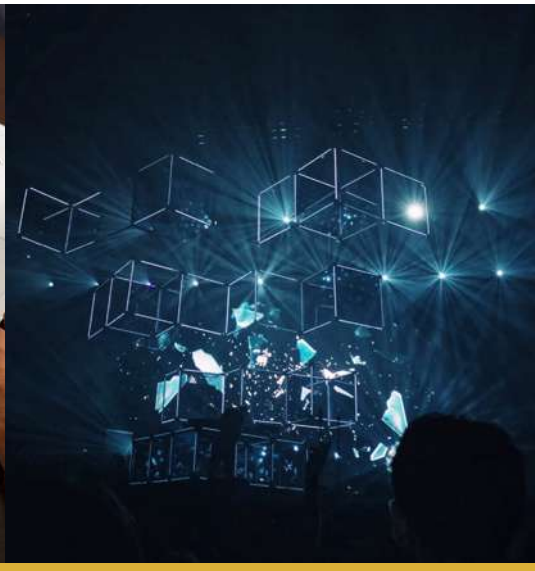
May 2021

DATA, INFORMATION & CYBER LAW

The Pangea DICL team is an international group of experienced and specialised lawyers dedicated to privacy, cybersecurity and open data issues. We support your digital transformation and guide you in the protection, use and defence of your immaterial assets from a legal perspective.

A multi-jurisdictional experts approach

A group of specialists familiar with their respective local laws and customs



A real curiosity and appetite for the latest technological developments & phenomena

EDITORIAL

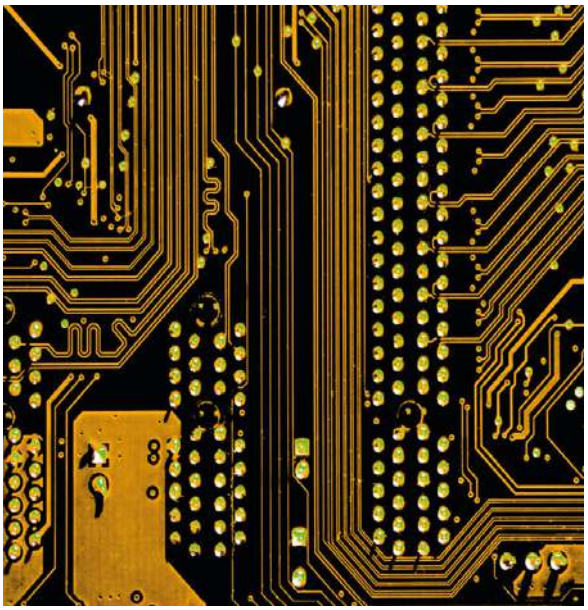
GDPR ENFORCEMENT - SIMILAR YET NOT THE SAME

PangeaNet is an association of independent law firms from over 25 countries forming an international law firm network. The Pangea Practice Group for Data, Information and Cyber Law consists of experts in IT and data protection law from around the world. In its bi-annual newsletter, the practice group provides information on relevant topics in this area such as current developments, national privacy regulations and the activities of regulatory authorities, as well as legal aspects of new technologies.

In the last year, the Pangea Practice Group for Data, Information and Cyber Law dedicated the first newsletter to the European General Data Protection Regulation (GDPR) and the second one dealt with the topic of Advertising Technology and its legal regulation as it is evergreen amidst the questions we hear every day, no matter the country. We will continue this scheme this year by introducing our potential clients to GDPR enforcement in our jurisdictions and block chain technology and its implications in the second half of this year.

Few days ago, the third anniversary of the entry of the world's most ambitious data protection regulation (GDPR) into force took place. As the level of national protection and people's awareness of the problem differentiated among member states, GDPR´s entry into force marked just the beginning of the long process of harmonisation. Therefore, the clients' focus shifted from the rules to their enforcement.

Because GDPR applies, for example in relation to the offering of goods or services, to the processing of personal data of all data subjects who are in the EU by entities not established in the EU, non-EU entrepreneurs are also interested in national enforcements.

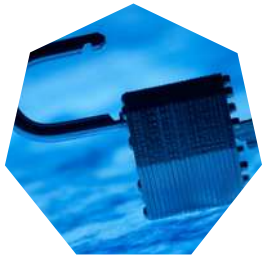


Therefore, we decided to provide the clients, as well as our non-EU colleagues, with short and practical overview of enforcement at least in jurisdictions in which members of this practice group are active.

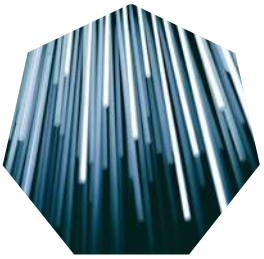
However, we hope that this newsletter will not be stiff and done job, but will continue to expand in the future.

Mgr. Bc. Tomáš Mudra
UEPA advokáti, Czech Republic

Index



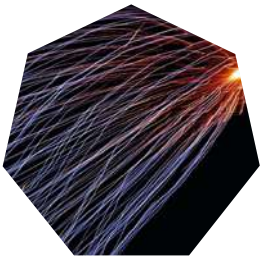
GDPR enforcement in Austria | 5



GDPR enforcement in Belgium | 7

GDPR enforcement in Bulgaria | 10

GDPR Enforcement in the Republic of Croatia | 12



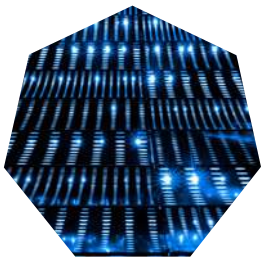
GDPR enforcement in the Czech Republic | 13

GDPR enforcement in France | 15

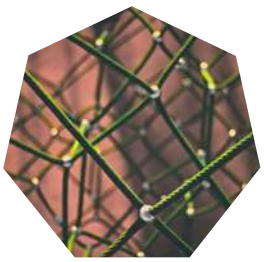
GDPR enforcement in Germany | 18

GDPR enforcement in Ireland | 20

GDPR enforcement in Italy | 23

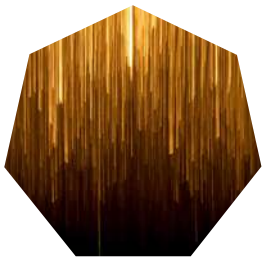


GDPR enforcement in Poland 24



GDPR enforcement in the Slovak Republic 28

GDPR enforcement in Spain 29



GDPR enforcement in Sweden 31

GDPR enforcement in the Netherlands 34

Members & Contacts 36

GDPR enforcement in Austria

NATIONAL DATA PROTECTION LEGISLATION AND DEROGATIONS FROM THE GDPR

After May 25, 2018, the General Data Protection Regulation (« *GDPR* ») and the revised national Austrian Data Protection Act (« *DPA* ») are the foundations of data protection law in Austria.

1) The Austrian data protection Authority

The Austrian Data Protection Authority ensures compliance with data protection in Austria. It has a monocratic structure, is independent due to European and international legal requirements, and is not subject to any official or professional supervision.

Austrian Data Protection Authority
Barichgasse 40-42
1030 Vienna.
Telephone: +43 1 52 152-0
E-mail: dsb@dsb.gv.at

> “
>
> THE DPA CONTAINS A « MEDIA PRIVILEGE » WHEN PROCESSING PERSONAL DATA FOR JOURNALISTIC PURPOSE.
>
> Anna Mertinz & Jennifer Held
> *KWR Karasek Wietrzyk Rechtsanwälte GmbH*

2) Some Austrian derogations from GDPR

In accordance with Art 85 GDPR the Austrian DPA introduces additional rules. Furthermore, case law in Austria contributes to the analysis and interpretation of the legal provisions. The following is a non-exhaustive overview of the Austrian specifics:

- Under Section 1 of the DPA, which is a constitutional provision, legal entities may also invoke protection of their personal data and enforce this protection by means of a complaint to the Austrian Data Protection Authority (Section 24 DPA). Furthermore, legal entities have certain rights (Section 1 para 3 DPA) such as the right to delete data.[1] Therefore, the DPA applies to legal entities, while the DPA **and** the GDPR apply to natural persons.

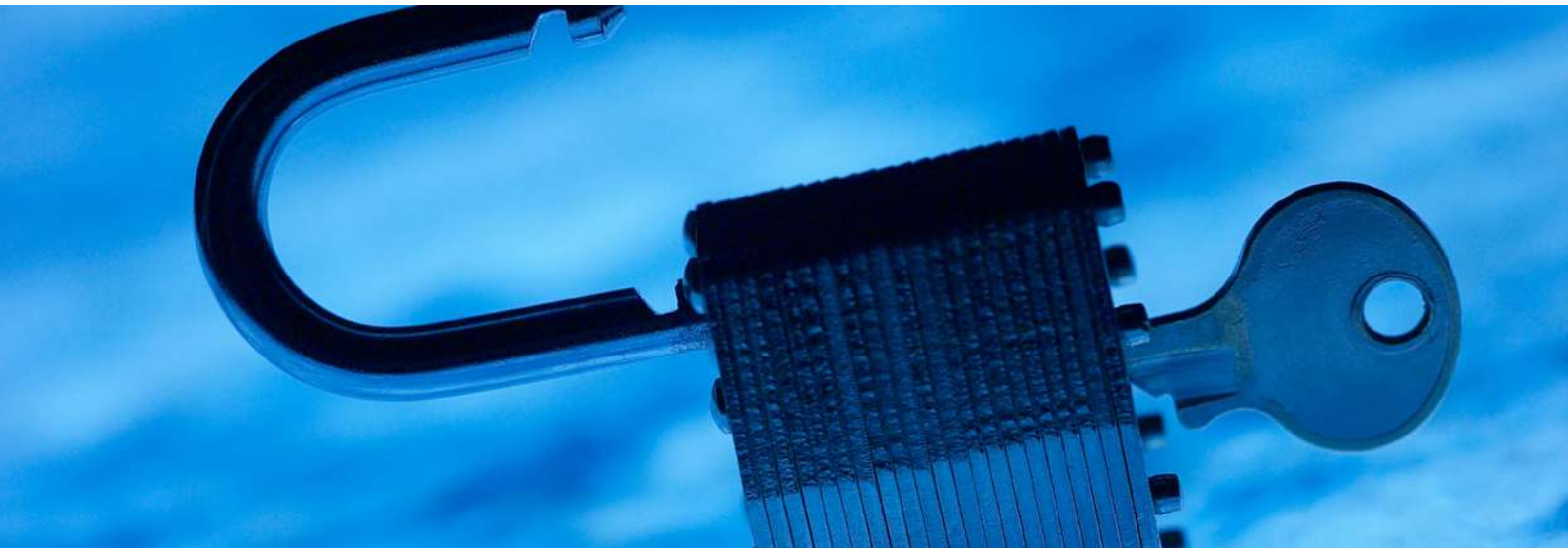
- The DPA contains provisions concerning the processing of personal data relating to acts or omissions subject to judicial or administrative penalties, including in particular the suspicion of the commission of criminal acts, as well as to criminal convictions or preventive measures.[2]

- The obligation to maintain data secrecy is mandatory and expressly stated in Section 6 of the DPA, i.e. concretizes Art 32 para 4 GDPR. The controller, the processor and their personnel – i.e. employees and individuals employed on an employment-like basis – must keep personal data arising from processing activities, which have been disclosed to them exclusively in connection with their professional activities or of which they have become aware, confidential to the extent there is no legal basis for the transfer of the personal data disclosed to them or of which they have become aware irrespective of any other legal confidentiality obligations (data secrecy). Personnel shall only transfer personal data based on an express instruction of their employer.

- Special rules apply to the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[3] In addition, the DPA contains a so-called « media privilege » when processing personal data for journalistic purposes by media owners, publishers and media employees or employees of a media company or media service.[4] This refers from Article 85 GDPR and extends the scope of the privilege to any processing of personal data for journalistic (para 1) or scientific, artistic or literary (para 2) purposes in accordance with Article 85 para 2 of the GDPR.

[1] For example mentioned in the decision of the Austrian Data Protection Authority from 20th May 2020 (DSB-D124.1182)
[2] See Section 4 para 3 Data Protection Act
[3] Section 7 Data Protection Act
[4] Section 9 Data Protection Act

• There are national rules for the imposition of fines towards a controller.[5] A legal entity is only liable to prosecution if a connection can be established between the actions of natural persons and the legal entity as a company. Therefore, the persons acting (mostly CEO) must be named and their actions must also be attributed to the legal entity. Hence, in deviation from Art 83 GDPR, which does not contain such requirement, the group of persons, whose violations trigger the criminal liability of the responsible person as a legal entity, is restricted according to national law. The Data Protection Authority has filed an extraordinary appeal against this ruling. The appeal proceedings are currently still pending before the Austrian Administrative Court.



3) Selected Austrian decisions

• On processing personal data of job candidates: If an applicant is rejected, the personal data in the form of the application documents have to be stored for 7 months after the rejection.[6] After the expiration of this period, the employer is obliged to delete the stored documents with personal data, unless otherwise provided by law.

• On "consent or money": A periodical offered its online users the opportunity to make a conscious decision as to whether they want their surfing behavior data to be analyzed and used for advertising purposes, or pay for the subscription without tracking (« consent or money »).[7] A complaint was filed and the Austrian Data Protection Authority ruled that the voluntary nature of the consent is nevertheless given. In addition, the Authority stated, since « consent » is not defined in the applicable Austrian Tele-Communication Law[8] it corresponds in a systematic interpretation to the term «consent» under Article 4 No. 11 or Article 7 GDPR, as follows from Article 94 para 2 GDPR. Accordingly, the assessment of whether consent has been given is to be made in accordance with the GDPR.

• On liability for damages: Austrian civil courts have made corresponding decisions in application of the GDPR. According to a judgment of the Vienna Regional Court regarding Facebook's liability for damages in the event of a violation of Article 15 of the GDPR, the social network company must pay damages of 500 euros because it failed to fulfill its obligations to provide information to Schrems. The company is also obliged to provide him with information about all personal data processed « free of charge and in full » within 14 days.

[5] Section 30 Data Protection Act
[6] Austrian Data Protection Authority, DSB-D123.085/0003-DSB/2018 from 27th August 2018
[7] Austrian Data Protection Authority, DSB-D122.931/0003-DSB/2018 from 30th November 2018
[8] The Tele-Communication Law [TKG 2003] takes precedence over Data Protection Act and GDPR as lex specialis

4) Sanctions and controls

According to the annual report of the Data Protection Authority[9] at the end of 2020, 47 part-time and full-time employees were working at the Data Protection Authority, including 32 lawyers (five of whom were interns), 4 staff members in the senior service and 10 staff members in the specialist service.

In the performance of their duties, the employees of the Data Protection Authority are bound by the instructions of the Director, Dr. Andrea Jelink. In 2020, 1603 individual complaints were filed at the Austrian Data Protection Authority, whereas 480 were discontinued and 852 were issued a decision.

All decisions of the Austrian Data Protection Authority can be appealed to the Federal Administrative Court. The court decides in a three-judge panel (one professional judge, two lay judges).

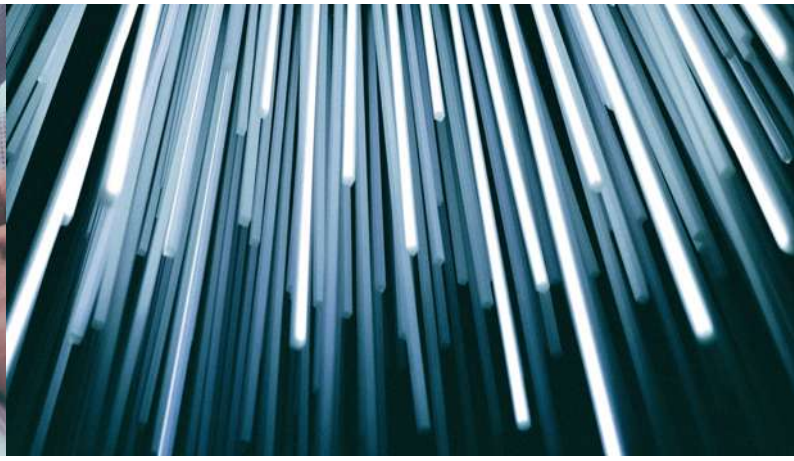
Decisions of the Federal Administrative Court may be appealed - also by the Austrian Data Protection Authority - to the Supreme Administrative Court or to the Constitutional Court.

5) Data protection officers - DPO

The relevant Articles of the GDPR (Art 37-39) and relevant recitals (91,97) apply. There are no national provisions regarding the designation of a DPO. The DPO has to comply with the obligation to secrecy when performing his tasks irrespective of any other confidentiality obligations.

Anna Mertinz & Jennifer Held
KWR Karasek Wietrzyk Rechtsanwälte GmbH

[9] See Datenschutzbehörde, Datenschutzbericht 2020, 4ff



GDPR enforcement in Belgium

The GDPR has been in force now for three years. As supervisory authorities across Europe are starting to apply a more active approach, the number of fines imposed increase at a very fast pace. In May 2020 the cumulative overall sum of fines amounted to approximately 110.00.000 €.

During the past year that amount increased with more than 250%. This trend is definitely visible in Belgium. In this contribution we will discuss the strategy of the Belgian supervisory authority for the next 4 years and the national derogations from the GDPR.

Course of overall sum of fines (cumulative)
Source: www.enforcementtracker.com

1) The national derogations from the GDPR

In Belgium, the legal framework that further implements the GDPR is mainly formed by the following two laws: the act of 3 December 2017 establishing the Belgian Data Protection Authority (« Gegevensbeschermingsautoriteit » or « GBA »)[1], further referred to as the BDPA Act, on the one hand and the act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data[2], further referred to as the DP Act, on the other hand.

The Belgian legislator decided to give priority to the reform of the national supervisory authority in its implementation, which resulted in the BDPA Act. The BDPA Act concerns the organisation of the Belgian Data Protection Authority.

From a business point of view and regarding the question how to proceed with the processing of personal data, the DP Act is particularly important. It can be partially described as the Belgian law implementing the GDPR, insofar as it deals with all the aspects which the GDPR requires or allows to be regulated by the Member States. As such, it is also the successor to the Personal Data Processing Act of 1992.[3]

On reading the DP Act, it is clear that in implementing the GDPR the Belgian legislator wanted to ensure continuity as much as possible and thus preserve the situation as it existed under the Personal Data Processing Act of 1992 (the so-called « policy-neutral approach »).

The most relevant derogations from and additions to the GDPR in the DP Act are:

• The limited cases in which the processing of personal data of a criminal nature is possible.[4]

• The processing activities that are considered to be necessary for reasons of substantial public interest, for example: the processing of personal data by associations with legal personality or foundations whose main statutory objective is the defence and promotion of human rights and fundamental freedoms and the processing of personal data concerning sexual life carried out by an association with legal personality or by a foundation whose main statutory objective is the assessment, support and treatment of persons whose sexual behaviour qualifies as a crime.[5]

• The Belgian legislator that entrusts the accreditation of certification bodies to BELAC, which is the national accreditation body that has been designated.[6]

• That the processing of the personal data of a child in relation to a direct offering of information society services to a child is lawful if the consent is given by children of at least 13 years old.[7]

• That article 83 of the GDPR (the imposition of administrative fines) does not apply to the government, unless it is a public-law legal person that offers goods or services on a market.[8] The latter addition is intended to ensure a « level playing field » in areas where the government is in competition with the private sector.[9]

• That some cases are mentioned in which it is appropriate to deviate from (certain) rights of the data subjects, mainly in matters relating to the fight against terrorism.[10]

• A number of conditions that are imposed on the processing of genetic, biometric and health data.[11]

2) The general praxis of the GBA regarding the enforcement of the GDPR

The Belgian Data Protection Authority (« Gegevensbeschermingsautoriteit » or « GBA », with its

[1] Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, BS 10 januari 2018, 989.
[2] Wet van 20 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, BS 5 september 2018, 68616.
[3] Wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens, BS 18 maart 1993, 5801.
[4] Article 10 of the DP Act, in execution of article 10 of the GDPR.
[5] Article 8 of the DP Act, in execution of article 9, §2 (g) of the GDPR.
[6] Article 18 of the DP Act, in execution of article 43 of the GDPR.
[7] Article 7 of the DP Act, in execution of article 8, §1 of the GDPR.
[8] Article 221, §2 of the DP Act.
[9] The Federation of Enterprises in Belgium (FEB) had reacted to this exception, which it considered contrary to the principle of equal treatment. Belgian legislation provides for very heavy administrative penalties in the event of non-compliance with the provisions of the GDPR, but in Belgium these penalties apply only to the private sector. The FEB thus sought the annulment of article 221, §2 of the DP Act and started a procedure before the Constitutional Court. In a judgement of 14 January 2021, the Constitutional Court rejected the appeal for annulment lodged by the FEB. The Constitutional Court confirmed the position of the Belgian legislator, considering that the need to ensure the continuity of the public service and not to jeopardise the performance of a mission of general interest justifies discrimination between public and private entities.
[10] Articles 11-17 of the DP Act, in execution of article 24 of the GDPR.
[11] Article 9 of the DP Act, in execution of article 9, §4 of the GDPR.

seat at BE-1000 Brussels, Drukpersstraat 35) is responsible for monitoring the compliance of the GDPR and other (national) legislation regarding data protection. Next to the GBA there are several « sector specific » supervisory authorities on the federal level, such as Comité P (the police supervisory committee) and Comité I (the standing committee on monitoring of the intelligence and security services).

On 28 January 2020 the GBA adopted the « strategic plan 2020-2025 ».[12] The GBA puts the emphasis on six strategic objectives and wants to improve data protection by:

1. Raising awareness: the GBA makes it clear that knowledge of data protection rights and obligations must be strengthened, so that a « privacy reflex » emerges among both data subjects and data controllers and a cultural shift can take place.

2. Enforcement: the GBA is changing from a purely advisory role as the « Privacy Commission » to a supervisory role as the Data Protection Authority. After all, the intention is that data subjets' rights will be respected in practice, not just on paper. In that respect, the GBA wishes to be an alert supervisor, whereby it will not only act proactively, but also reactively.

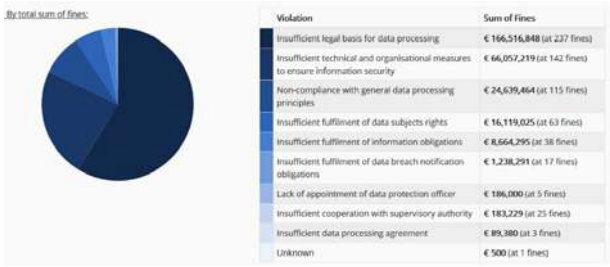
3. Identifying and responding to evolutions: certain phenomena, such as (the development of) new technologies, have an impact on data protection. It is therefore important to (co-)monitor, understand and correctly assess technological, economic and social developments so that the GBA can keep its finger on the pulse and respond appropriately.

4. Cooperation: this cooperation can be national and/or international. Data protection in a globalised society must be tackled jointly according to the GBA. Being a reliable partner for other data protection authorities is extremely important for the GBA in this global world. The GBA cooperates with other authorities, for example, in the area of complaint handling.

5. Being a leader/guide and reference centre: this objective further indicates the GBA's desire to act as a recognised leader and reference centre for data protection. The intention is that it is a trusted party, known for its professionalism.

6. Being an efficient supervisor: the GBA will critically analyse its current organisation and pay (more) attention to a « systematic » and flexible approach to its activities. On the one hand, it will have to have the ability to deal with social and technological changes. On the other hand, the GBA will need to be flexible in order to be able to pay attention to the multitude of its tasks within the budgetary margin, whereby the workload will depend on external factors.

In its strategic plan the GBA also sets out 3 categories of priorities, in addition to a range of operational tasks that the GBA is legally required to perform. Firstly, the priority sectors are identified: telecommunications and media, government, direct marketing, education and SME's. The second category of strategic priorities includes three instruments from the GDPR that are considered to be important building blocks for better data protection: the role of the Data Protection Officer (DPO), the legitimacy of the processing of personal data and the rights of data subjects (access to, rectification of, transfer of personal data, etc.). Finally, the third category includes subjects that are high on the social agenda: pictures and cameras, online data protection and sensitive data.



Those priorities can already be derived from the sanctions imposed by the national data protection autorities. For instance, an insufficient legal basis for data processing is by far the most important violation that led to a fine. The insufficient fulfilment of data subjects rights and the lack of appointment of a DPO are also present in the top 10.[13]

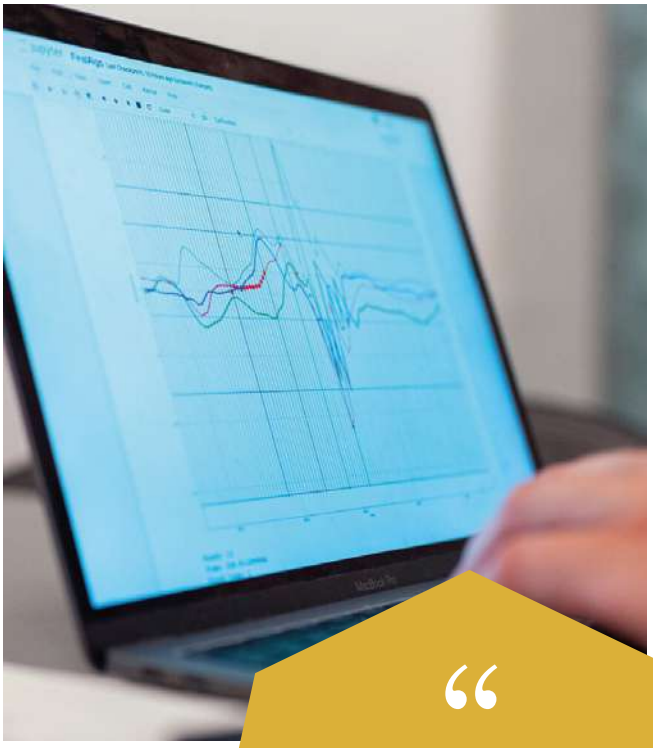
Litiguard Law Firm provides different types of services to make sure its clients become and remain GDPR compliant. Next to drafting and reviewing all kinds of compliance documentation (such as (privacy) policies, records of processing activities and data protection impact assessments) and advising our clients on specific processing activities and business cases that entail the processing of personal data, we also offer high level DPO services.

Michiel Beutels
Litiguard Law Firm

[12] https://www.gegevensbeschermingsautoriteit.be/publications/strategisch-plan-2020-2025.pdf
[13] Source: www.enforcementtracker.com

GDPR enforcement in Bulgaria

National Data Protection legislation and derogations from the GDPR



Generally, the Bulgarian Personal Data Protection Act (PDPA) reflects the provisions of the GDPR. The PDPA either develops the provisions of GDPR, in the cases permissible, or introduces new rules in accordance with the derogations under Art. 85 of the Regulation.

The main new rules to the regulations of the GDPR are contained in Art. 25 of the PDPA, such as:

1/ When personal data is provided by the data subject to an administrator or processor without legal grounds under Art. 6, para. 1 of GDPR or in contradiction with the principles under Art. 5 of the same Regulation, within one month from the knowledge the controller or the processor is obliged to return the personal data, and if this is impossible or requires disproportionately large efforts, to delete or destroy it and to document this.

> “
>
> COMPLAINTS FILED IN 2020 ARE CHARACTERIZED BY LEGAL AND FACTUAL COMPLEXITY.
>
> Nikolay Belokonski
> *KWR Belokonski Gospodinov & Partners*

2/ Along the general obligation of the controllers and the processors under Art. 37, para. 7 of GDPR, the PDPA imposes on them an obligation to notify the Commission for Personal Data Protection (CPDP) of « the names, the unique civil number or the personal number of a foreigner, or other similar identifier and the contact details of the DPO, as well as subsequent changes in them », and in addition the form and content of the notification, as well as the procedure for its submission is determined by a separate sub-legislation.

3/ The age limit for lawful processing of personal data of children is 14 years.

4/ An administrator or processor may copy an identity document, a driving license or a residence document only if required by law – this is meant to limit this widespread practice. The same applies also for the free public access to the unique civil number or the personal number of a foreigner, which is also restricted. It is therefore prohibited to require or preset the unique civil number or the personal number of a foreigner as PIN code for access to administrative online services.

5/ There are additional requirements for a processing on a large scale of personal data, including video surveillance, according to which administrators / processors must adopt special rules for processing.

6/ Special rules are provided for the processing of personal data for journalistic purposes, as well as for academic, artistic or literary expression.

7/ There are also a few specific provisions regulating processing of personal data of employees. In the following cases the employer is obliged to adopt special rules and procedures: (i) use of a system for reporting of violations; (ii) restrictions on the use of internal company resources; (iii) introduction of systems for access control, working hours and labor discipline. Further, the period for storage of personal data of job candidates may not be longer than 6 months, unless the candidate has given her/his consent for storage for a longer period.

After the expiration of this period, the employer is obliged to delete or destroy the stored documents with personal data, unless a special law provides otherwise. Where, in a recruitment procedure, the employer has requested the provision of originals or notarized copies of documents certifying the candidate's physical and mental fitness, the required qualifications and seniority for the position, the employer is obliged to return those documents to the data subject, who is not approved for the job, within 6 months from the final completion of the procedure, unless a special law provides otherwise.

Data protection authority

The data protection authority under GDPR in Bulgaria is the CPDP with seat at 2 Prof. Tsvetan Lazarov Blvd., Sofia 1592, which does not have any local branches. It is also vested with the supervision of data security under the Electronic Communications Act, which regulates the sending of advertising mail such as electronic newsletters and advertising e-mails.

Sanctions and controls

Inspections are carried out by the CDPD a) based on its annual plan made by the CDPD or b) uponcomplaints or communications about personal data law breaches delivered to the CDPD.

In 2020, the CDPD was approached with over 680 complaints filed by individuals, alleging violations in the processing of personal data and the exercise of rights. There is a smaller number of complaints compared to the previous 2019 and 2018, when the number of complaints for 2019 exceeds 1600, and for 2018 is over 780. Complaints filed in 2020 are characterized by legal and factual complexity, including the intervention of an international element, complainants who are not Bulgarian citizens or data controllers with a main place of establishment outside the territory of the Republic of Bulgaria, as well as non-individualized by the complainants respondent parties, most often administrators of electronic sites, a circumstance that also requires cooperation with the bodies of the Ministry of Interior to establish the latter.

The DPA evaluates the information provided by the complainant and in case of less severe breaches, the DPA sends a so-called communication regarding a potential breach of data protection law to the controller.

In case of more severe or undisputable breaches or if the controller takes no satisfactory remedial action by himself, the DPA starts official administrative proceedings and carries out an investigation and inspects the controller. In 2020, based on well-founded complaints, mainly corrective measures under Art. 58, para. 2 of GDPR were imposed, whereas mainly under lit. d) and i) thereof. In 2020, sanctions in the total amount of BGN 518,700 were imposed for established violations of GDPR and PDPA in the proceedings for review of complaints and signals.

DPO

In the practice and among controllers, there is still a misunderstanding about the hypotheses, under which controllers and processors are obliged to appoint a DPO. Nevertheless, this kind of services is provided by a wide spectrum of subjects. The CDPD has published Instructions on the fulfilment of the obligation of the controllers and the processors to notify the CPDP when appointing a DPO. Further, the CDPD also published the Guidance for data protection officers in the public and quasi public sectors on how to ensure compliance with the European Union General Data Protection Regulation (The DPO Handbook).

There are no additional rules or guidelines nor any professional chamber. Law firms usually provide DPO services not directly, but via an affiliated company due to the fact that standard professional insurance of law firms does not cover the activities of a DPO and due to potential conflicts of interests.

Nikolay Belokonski
KWR Belokonski Gospodinov & Partners

• CROATIA

GDPR Enforcement in the Republic of Croatia

Croatian Personal Data Protection Agency ("AZOP")

As an administrative authority, AZOP is subject to other national laws regulating administrative procedures and disputes (i.e., decisions made by AZOP are subject to appeal before the Croatian Administrative Courts). AZOP publishes resolutions and opinions in regard to the processing of personal data, initiates administrative procedures and performs supervision over private persons and other public authorities, issues monetary fines for breaches of personal data protection provisions, et al. Certain aspects of data privacy in specific areas are also enforced by other competent authorities. For example, - Croatian Regulatory Authority for Network Industries (« HAKOM ») — in which competence is Electronic Communication Act supervises and enforces provisions related to unsolicited communications, as well as the use of cookies.

Specific National Rules

i. In relation to the offer of information society services directly to a child, the processing of the personal data of a child is lawful only where the child is at least 16 years old;

ii. The processing of genetic information is forbidden for the purposes of calculating the probability of illnesses when entering into specific agreements in the field of insurance;

iii. The processing of biometric data in the private sector is permitted only where expressly envisaged by law, or in cases where it is required for the protection of persons, assets, classified data, business secrets or for individual and definite identification of the users of services.
The processing of biometric data of employees is permitted only for the purpose of recording working time and for entry/exit records to/from business premises, if stipulated by law or if such processing is an alternative to other means of recording such information. In both cases, the legal ground for the processing of biometric data in the latter case must always be the consent.
Provisions on processing of biometric data are applicable to data controllers with the business establishment in Croatia or which provide services on the territory of Croatia, as well as to public authorities;

iv. The processing of personal data by means of video surveillance may be performed only for a purpose which is necessary and justified for the protection of persons and assets. The Implementation Act also defines which parts of a buildings and space (as well as which spaces controllers are prohibited to surveil) may be subject to video surveillance and the obligation of the data controllers or data processors to clearly indicate (by means of a sticker or similar) that certain object is under video surveillance, as well as the information that need to be included in the respective notice.
Only the responsible person of the data controller or the person authorized by the responsible person may have the right of access to video surveillance recordings. Data controller and data processor are required to establish an automated log system to video surveillance recordings. The video surveillance recordings may be kept for the maximum period of 6 months, except in certain exceptional cases (e.g., evidentiary purposes in court proceedings).

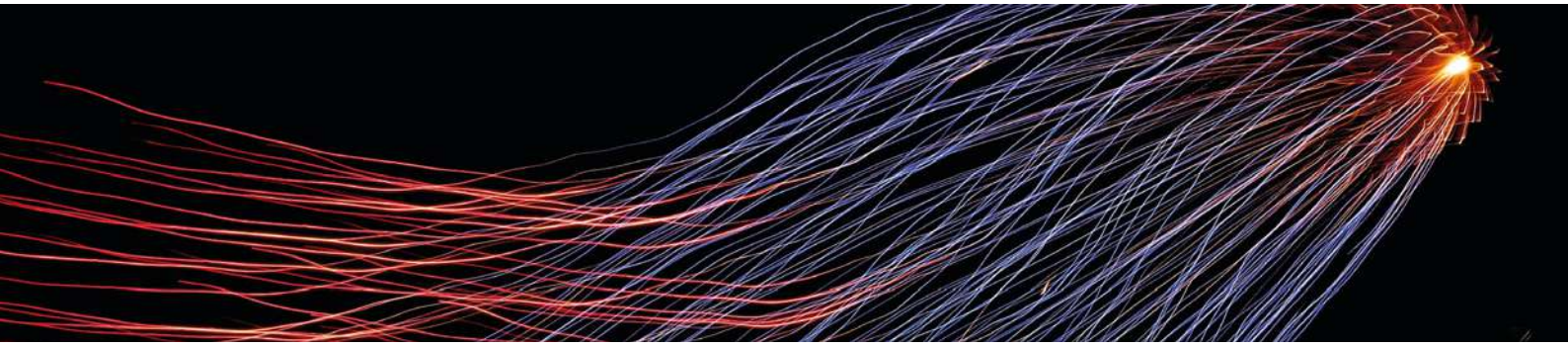
Enforcement

Until recently, AZOP has been more focused on educating with respect to the GDPR, and less on supervisions for compliance and issuing of fines. However, recently a first fine was issued to a bank for repeated non-compliance with the requests of data subjects for access to their data. The bank claimed that it is not required to provide a copy of the documentation related to loans given by the bank to data subjects. The bank argued that it is not personal data, but rather documentation required to be kept under banking regulations. AZOP found such position of the bank to be contrary to the provisions of GDPR and after ordering the bank to disclose such data on several occasions, decided to fine the bank. Although the amount of the fine is not public, according to the information available in data protection community, the fine was HRK 1,1 million (app. 150,000 €).

Regarding cookies, in November 2019, HAKOM issued a decision in which it confirmed the position taken by the ECJ in Case No. C-673/17 regarding the standard of consent in relation to use of cookie technology. HAKOM considers that an effective consent requires an unambiguous action of confirmation, such as actively clicking a box affirming consent on a website. Accordingly, cookie banners which seek to establish consent simply through a user continuing surfing on a website are not admissible. In the same decision, a telecom provider was ordered to comply with said requirements, under the threat of a monetary fine.

In case of livestreaming of public spaces, the deciding factor on whether or not the Implementation Act applies is the possibility of storage of the relevant video footage. If there is no storage system, i.e., if there is no possibility of accessing the footage after the livestream ends, the Implementation Act does not apply, therefore, such livestreaming is outside the scope of the Implementation Act. However, if such a storage space exists, regardless of the geographical location of the storage, video surveillance of public spaces is only allowed for public legal persons or legal persons with public authorities, as well as only in cases permitted by the law, if such surveillance is necessary for fulfilment of tasks and obligations of public authorities and for the protection of the lives and health of persons and property.

Andrea Kožul Pediši & Marko Kneževi
Vukmir and Associates



CZECH REPUBLIC •

GDPR enforcement in the Czech Republic

Personal data protection law plays much more significant role in day-to-day life and activities than ever before. In the Czech Republic enforcement of GDPR was a big topic 2 years ago, but t in the end it has not become such a tough and problematic area as some expected.

National data protection legislation and derogations from the GDPR

The Czech Personal Data Protection Act mainly regulates questions regarding personal data processed by the public sector or in the public interest. It provides only the following specification with any practical impact on personal data processing in the private sector:

- the age limit for lawful processing of personal data of children is 15 years.
- the controller may inform about the rectification, erasure or restriction of processing of personal data just by changing the content of the respective filing system, if it is regularly made available to the data subjects.

• the controller does not need to make a data protection impact assessment if the data processing in question is required by law (or for purposes stated by law).

Regarding the special processing situation, there are a few specific provisions of the Labour Act regulating processing of personal date of employees. They enable the employer to request and process within the recruitment process such information including personal data of job candidates, which is immediately connected to the work offered, and stipulates a general ban on such monitoring of employees, which might invade their privacy (i.e. monitoring of communication made via work email or of the employees´ online activities) and exemptions thereof.

Data protection authority

The only data protection authority under GDPR in the Czech Republic is the Office for Personal Data Protection (DPA) with seat at Pplk. Sochora 27, 170 00 Praha 7, Czech Republic, which does not have any local branches. It is also vested with the supervision of bulk commercial communications under the applicable national laws and EU regulations.

Sanctions and controls

Inspections are carried out by the DPA a) based on its annual plan made by the DPA in advance with the aim of cross-sectional inspections or b) upon complaints or communications about personal data law breaches delivered to the DPA. In 2020, the DPA carried out 54 inspections.

Unless planned in advance, inspections and proceedings are started by the DPA upon a complaint by a data subject, that the law was breached. Collective actions or complaints made in favour of data subjects by associations are not allowed. The DPA evaluates the information provided by the complainant and in case of less severe breaches, the DPA sends a so-called communication regarding a potential breach of data protection law to the controller.

> “
>
> ONLY A SMALL PORTION OF INSPECTIONS HAS BEEN CONCLUDED BY A FINE.

In case of more severe or undisputable breaches or if the controller takes no satisfactory remedial action by himself, the DPA starts official administrative proceedings and carries out an investigation and inspects the controller. Except in cases of obvious grave breaches of data protection law, inspections are generally concluded by the statement that the breach was remedied during the inspection or that remedial action was officially imposed, which was performed by the controller later. Only a small portion of inspections has been concluded by a fine - on average in the amount not higher than 3000 €. The highest fine imposed so far, for a repeated and flagrant breach of law, was around 230.000 €.

DPO

In practice, this kind of services is provided by a wide spectrum of subjects. There are no additional rules or guidelines nor any professional chamber. Law firms usually provide DPO services not directly, but via an affiliated company due to the fact that standard professional insurance of law firms does not cover the activities of a DPO and due to potential conflicts of interests. We have such affiliated company, which provides services of a DPO as well as a representative of processor or controller under Art. 27 of GDPR.

Tomáš Mudra
UEPA Advokáti s.r.o.

GDPR enforcement in France

Before the enforcement of the GDPR, 3 years ago, the data protection legal framework in France, implemented over 4 decades, was one of the most developed in Europe and the CNIL (the French Data Protection Authority) was already very active in terms of investigations, even if the sanctions were not as substantial as today. Therefore, the French legislator decided not to abrogate the French Data Protection Act (Law No. 78-17 of 6 January 1978, hereinafter « **FDPA** ») but to amend it[1] to bring national law into line with the GDPR.

Data protection authority

The data protection authority in France is the « Commission Nationale de l'Informatique et des Libertés » or the « CNIL ». The CNIL, composed of around 200 employees, is located at 3 Place de Fontenoy, 75007 Paris and does not have any local branches.

The CNIL is an independent administrative authority whose missions are to inform, advise, investigate and sanction. Therefore, the CNIL issues a lot of guidelines every year, available on its website, on different topics concerning processing of personal data (e.g., recommendations and guidelines on cookies issued on 17 September 2020).

National derogations from the GDPR

a. Rights and data protection of data subjects

The French legislator has used the margin of manoeuvres provided by the GDPR for the Member States to strengthen the rights and protection of data subjects' personal data. Therefore, the FDPA specifies that:

- the consent of a child for the processing of his/her personal data in relation to information society services is lawful if the latter is of at least 15 years old[2];
- two procedural innovations are introduced: (i) class action for damages (where several data subjects suffered harm as a result of similar breach of data protection law by a controller or a processor)[3], and (ii) action by mandatary (a data subject mandating an association or a trade union to bring action in the CNIL or courts)[4];
- each data subject may define general or particular guidelines regarding the retention, deletion and communication of his or her personal data after death[5].

[1] The FDPA was amended with the Law No. 2018-493 of 20 June 2018, the Decree No. 2018-687 of 1 August 2018 and the Decree n°2019-536 on 30 May 2019.
[2] Article 48 of the FDPA, in execution of the article 8, §1 of the GDPR.
[3] Article 37 of the FDPA, in execution of article 80, §2 of the GDPR. A class action can be brought by (i) an association existing for at least 5 years, whose statutory purpose included the defence of the privacy and data protection, (ii) an approved consumer association (e.g., UFC-Que-Choisir, CNAFC, CNL, etc.), and (iii) certain trade union organisations. The CNIL must be informed by the applicant and a class action can only concern facts happening after the 25 May 2018. Furthermore, a class action may only be brought in competent administrate or civil courts.
[4] Article 38 of the FDPA, in execution of article 80, §1 of the GDPR. An action by mandatary can be brought by the same associations and trade unions than the ones provided for a class action.
[5] Article 48 of the FDPA.

However, the FDPA also provides some restrictions of data subjects rights. Hence, the right to be informed does not apply when (i) the personal data have not been obtained from the data subject and the processing is carried out on the behalf of the French State and is related to public security, or (ii) the processing is carried out by tax public administrations[6]. In addition, the right to access, erasure and rectification is restricted for processing carried out by tax public administrations (and also by financial courts in the context of their non-judicial tasks concerning the right to access) or for processing carried out for public security[7].

b. Specifications for the controllers and processors

The FDPA also provides derogations from and additions to the GDPR regarding the obligations of the controller and processor, where the more relevant are the following:

- the processing of health data can be based on additional legal basis than the ones provided in the GDPR[8]:
  - processing necessary for preventive medicine, medical diagnostics and management of health services;
  - employers may process biometric data to the extent that strictly necessary to control access to premises, equipments or applications used in the context of tasks entrusted to the employer's personnel or services providers provided that the employer comply with the data standards issued by the CNIL;
  - the use of public information contained in the court decisions that could contain sensitive data is allowed to the extent that the purpose or the effect of the re-identification of the data subject is not possible[9];
  - the processing of sensitive data may be carried out for the purposes of public research, public interest or statistical by a specific French Institute;

- except for certain processing (e.g., preventive medicines processing, etc.), the processing of health data must comply with CNIL's data standards or require a prior authorization from the CNIL[10];
- the processing of data related to criminal offences or convictions may be carried out for the purposes of legal proceedings and enforcement by a specific list of individuals and by public authorities[11];
- the processing of national identification data must be authorized by a decree of the State Council (Conseil d'État[12]) except if the processing is carried out for statistical, scientific, historical research or online government services purposes[13];
- the administration is allowed to take an individual administrative decision solely based on automated processing, provided that, such processing does not concern any sensitive data and the automated decision does not concern an administrative complaint[14];
- the processing of personal data carried out on behalf of the French State for the purposes of (i) national security or public safety, or (ii) prevention, investigation, detection, prosecution or enforcement of criminals offences or safety measures, must be based on an order of the competent minister(s) (or Decree of the State Council (Conseil d'Etat) if sensitive data are concerned), after CNIL gives opinion[15].

[6] Article 48 of the FDPA, in exécution of article 23 of the GDPR.
[7] Article 58 of the FDPA, in execution of article 23 of the GDPR. Note also that the obligation of notification of personal data breach to data subjects is not mandatory if such notification would constitute un risk for national security (Article 58, II of the FDPA, in execution of article 23 of the GDPR).
[8] Article 44 of the FDPA, in execution of article 9, §4 of the GDPR.
[9] The regime for making court decisions available to the public in electronic form, « open data », was specified by Decree No. 2020-797 oon 29 June 2020, followed by an Order on 28 April 2021. The open data of the court decisions will start from September 2021. The names and surnames of the parties or third parties mentioned in the decision will be systematically erased.
[10] Article 66 of the FDPA, in execution of article 9, §4 of the GDPR.
[11] Article 46 of the FDPA, in execution of article 10 of the GDPR.
[12] French administrative supreme authority.
[13] Article 30 of the FDPA, in execution of article 87 of the GDPR.
[14] Article 47 of the FDPA, in execution of article 22, §2 of the GDPR.
[15] Article 31 of the FDPA

It is also important to note that, pursuant to article 35(4) of the GDPR, the CNIL has issued a list of 14 processing activities subject to a mandatory impact assessment[16] (e.g., processing for the purpose of constantly monitoring the activity of the employees, large-scale geolocalisation processing) and a list of 14 processing activities not subject to[17].

Sanctions and controls

The CNIL's investigations may be based on its annual priority plan or upon complaints received, and they also may be part of joint operations with other European supervisory authorities. In its 2021 annual priority plan, the CNIL has indicated that its controls and sanctions will be focus on 3 priority areas: cybersecurity, health data security and use of cookies.

The CNIL is empowered to control all private companies, associations or public organizations that process personal data on the French territory. The first stage is the investigation that can be conducted on-site and/or online. Except for the correspondence between a lawyer and his clients or data covered by the secrecy of journalistic processing, the professional secrecy cannot be invoked by a processor or a controller against the CNIL in the framework of its investigation[18]. Furthermore, the CNIL can investigate online under an assumed identity[19].

At the end of the investigation, the CNIL can decide to close the investigation proceeding if the controller or the processor comply with the provisions of the GDPR. However, if breaches have been identified, the CNIL can decide to (i) give a warning, or (ii) issue a formal notice to implement measures, within a given period of time, in order to cease the breaches, or (iii) impose sanction(s) (e.g., a reprimand, a temporary or definitive limitation to the processing, an administrative fine whose amount is determined on elements mentioned in the article 83 (5) and (6) of the GDPR, etc.)[20]. Furthermore, the CNIL can decide to make its decision public.

Decisions of the CNIL may be appealed to the State Council (Conseil d'Etat) within 2 months of the notification or the publication of the decision.

Only for the 2020 year, CNIL has imposed 14 sanctions and 49 orders to comply. The CNIL does not hesitate to impose hefty fines: it is the first European Authority to sanction a GAFA such as Google LLC and Google Ireland fined respectively 60m and 40m on 7 December 2020 for depositing cookies without valid consent. The same day and for the same reasons, the CNIL also sanctioned Amazon Europe Core with a fine of 35m. The CNIL also sanctions French compagnies such as Carrefour Banque and Carrefour France which were fined 2.250m and 800K because of several GDPR's violations on 7 December 2020[21].

Matthieu Bourgeois & Laurent Badiane
klein • wenner

[16] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf
[17] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf
[18] Article 19 of the FDPA. Under certain conditions, the medical secrecy can be invoked against the CNIL. 19 Article 20, III of the FDPA.
[20] Article 20 of the FDPA.
[21] A table of the sanctions issued by the CNIL in 2019 and 2018 is available on the CNIL's website: https://www.cnil.fr/en/sanctions-issued-cnil

• GERMANY

GDPR enforcement in Germany

With the entry into force of the General Data Protection Regulation (GDPR), the protection of personal data has become more important in many German companies. The future enforce-ment of the GDPR was eagerly awaited before its applicability began on 25 May 2018. In the meantime, about three years later, there are already a large number of regulatory proceedings and court decisions in Germany that deal with the GDPR, as well as national laws that supple-ment or deviate from the GDPR.

National data protection regulations

The national data protection regulations in Germany are contained in particular in the Federal Data Protection Act (BDSG). With the new version of the BDSG as of 25 May 2018, the German legislator has made use of some of the opening clauses of the GDPR and provided for individ-ual regulations that deviate from or supplement the GDPR. Essential regulations are, for example, the following:

- Section 26 of the BDSG stipulates that the processing of employee data is permissible, among other things, for the purpose of establishing, implementing and terminating an employment relationship.

- Sections 32-37 BDSG standardize reasons for the restriction of data subjects' rights.

- Section 38 of the BDSG requires the appointment of a data protection officer if the controller or processor generally employs at least 20 persons on a permanent basis for the automated processing of personal data.

- Sections 41-43 BDSG contain regulations on sanctions, in particular penalties and fines.

In addition, there are other regulations that relate primarily to special data processing situa-tions. One of the relevant laws is the German Art Copyright Act (KunstUrhG). An important regulation is section 22 p. 1 KunstUrhG, according to which portraits may only be distributed or publicly displayed with the consent of the person portrayed. On 10 February 2021, the German Cabinet passed a draft law on data protection and privacy in tele-communications and telemedia (TTDSG). Among other things, this is intended to include the consent requirement for technically unnecessary cookies in the text of the law.

Data protection supervisory authorities

At the national level, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) is responsible for the supervision of federal public bodies as well as companies, insofar as they process data of natural or legal persons for the businesslike provision of tele-communication services (Section 9 (1) BDSG). It has its registered office at Graurheindorfer Str. 153, 53117 Bonn, Germany.

In addition, there is a data protection supervisory authority in each of the federal states, which monitors compliance

with data protection at public bodies in the state as well as at non-public bodies that have their registered office in the respective federal state. Their contact details can be found on the BfDI's website.

Due to the jurisdictional regulations, the BfDI's activities are generally of no factual significance for companies. Depending on the respective federal state, the individual state data protection authorities are responsible for companies. In some cases, these authorities handle data pro-tection issues differently, which means that in Germany a situa-tion can be assessed differently depending on the federal state and the responsible data protection supervisory authority.

Investigations and sanctions by data protection supervisory authorities

The data protection supervisory authorities act on an ad hoc basis, for example in the context of spot checks in companies, as well as on an ad hoc basis on the basis of complaints and inquiries from data subjects. According to the BfDI's 2020 activity report, it had received 7,878 complaints and inquiries from citizens in 2020. The agency had also received 10,024 data breach notifications.

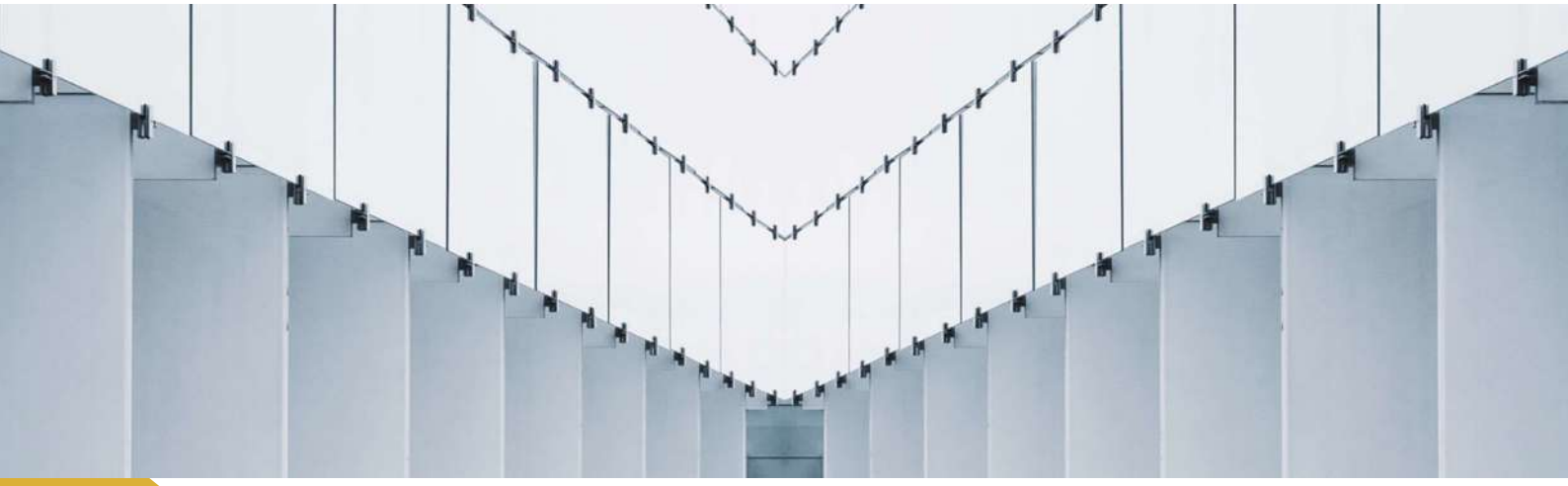
The Data Protection Conference (DSK), the association of the data protection authorities of the German states and the federal government, published its concept for the assessment of fines in proceedings against companies within the scope of the GDPR in October 2019. The main point of reference for the amount of the fine is the annual turnover of the last financial year; in addition, the « gravity of the offense » is decisive for the amount of the fine.

The highest fine for data protection violations in

> IN ADDITION TO THE BFDI, THERE IS A DATA PROTECTION SUPERVISORY AUTHORITY IN EACH OF THE FEDERAL STATES.

Germany to date was imposed by the Hamburg Commissioner for Data Protection and Freedom of Information in the amount of approx-imately 35.3 million euros on H&M Hennes & Mauritz Online Shop A.B. & Co. KG. The company was accused of extensive monitoring of employees.

Some companies were able to successfully de-fend themselves against the fines imposed. For example, the Bonn Regional Court reduced the amount of a fine of 9.55 million euros imposed by the BfDI on 1&1 to 900,000 euros. In another case, the Berlin Regional Court deemed the fine of 14.5 million issued by the Berlin data protection supervisory authority against Deutsche Wohnen SE to be invalid for formal reasons. In the opinion of the court, sanctioning the company is out of the question insofar as no fault on the part of management personnel can be proven against the company. The question of whether the internal responsibilities of a legal entity must be clarified



in order to impose a fine despite the existence of a data protection violation is relevant to the practice of all German data protection supervisory authorities in imposing fines. If the answer is in the affirmative, this would mean that in large companies it would often not be possible to prove responsibility and thus - in contrast to other EU countries - a fine could not regularly be imposed in Germany. In agreement with the Berlin data protection authority, the Berlin public prosecutor's office has filed an appeal against the court's decision.

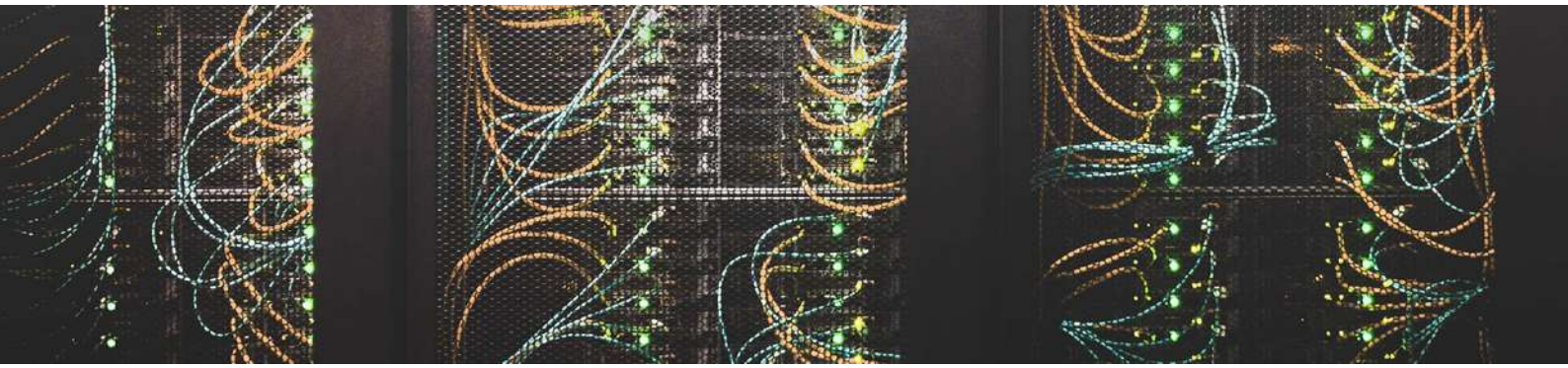
Further clarification of the relationship between national administrative offence law and European data protection law therefore remains to be seen.

Data Protection Officer

The function of data protection officer can be assigned to the lawyer who represents the company in legal matters in this area anyway. In this respect, there is no prohibition of activity under professional law. The regulations governing conflicts of interest in Germany (cf. Section 45 (1) No. 4 of the Federal Lawyers' Act) primarily cover cases in which the lawyer is acting in a secondary profession. However, the lawyer will not provide advice on data protection issues in addition to his work as a lawyer, but will perform this task precisely as a lawyer, so that there is no second profession in this sense.

Like some other law firms, we offer this service accordingly for our clients and see the advantage that not only pure advice can be covered, but also, if necessary, a contentious dispute with other parties and authorities.

Dr. Sebastian Meyer & Johanna Schmale
BRANDI Rechtsanwälte



GDPR enforcement in Ireland

National data protection legislation

In Ireland, the national law which gives further effect to the GDPR is the Data Protection Act 2018 (« DPA 2018 »). The DPA 2018 repeals the Data Protection Acts 1988 to 2003, except for provisions relating to the processing of personal data for the purposes of national security, defence and international relations of the State. The collective citation is now « the Data Protection Acts 1988 to 2018 ».

If a data protection infringement or complaint relates to an incident that occurred before 25 May 2018, the Data Protection Act 1988 and the Data Protection Act 2003 will apply. After 25 May 2018, the GDPR applies.

Ireland has a written Constitution. While it does not specifically guarantee a right to privacy, courts in Ireland recognise that the personal rights set out in Article 40.3 of the Constitution of Ireland imply a right to privacy.

In Ireland, the processing of personal data in the electronic communications sector is governed by the GDPR's general rules and the specific rules of the European Communities (Electronic Communications Networks and Services) (Privacy And Electronic Communications) Regulations 2011 (2011 E-Privacy Regulations).

Derogations from the GDPR

1. Data Subject Rights

The DPA 2018 provides that data subject rights provided for under Articles 15, 16, 18, 19, 20 and 21 of the GDPR may be restricted where personal data is processed for:

- Archiving purposes in the public interest; and
- Scientific or historical research purposes or statistical purposes.

Where personal data is processed for the above purposes, data subject rights may only be restricted if:

- The exercise of those rights would likely render impossible, or seriously impair, the achievement of those purposes; and
- Such restriction is necessary for the fulfilment of those purposes.

2. Children

Any references to a 'child' in the GDPR should be taken to refer to a person under the age of 18 years. The DPA 2018 however has set the age of digital consent at 16, which means that if an organisation is relying on consent as the legal basis (justification) for processing a child's personal data and the child is under 16, then consent must be given or authorised by the person who has parental responsibility for the child.

The DPA 2018 provides a specific right of erasure for children in respect of data collected pursuant to the provision of information society services. A controller must, at the request of the data subject, without undue delay, erase personal data of the data subject where the data has been collected in relation to the offer to that data subject of information society services.

3. Processing of special categories of data

Article 9 of the GDPR gives Member States some flexibility with respect to the lawful bases to legitimise the processing of special categories of data. The DPA 2018 permits the processing of special categories of personal data in the following circumstances:

- If the processing is necessary and proportionate:
  - in preventing a threat to national security, defence or public security, or preventing, detecting, investigating or prosecuting criminal offences;
  - for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, legal proceedings or prospective legal proceedings;
  - for the administration of justice or the performance of a function conferred on a person by or under an enactment of by the Irish Constitution;
  - for the purposes of a policy of insurance or life assurance, a health insurance policy, a pension arrangement or mortgaging of property.
- Where processing is carried out in the course of electoral activities in Ireland for the purpose of compiling data on peoples' political opinions by a political party or by a candidate/holder of elective political office in Ireland, and by the Referendum Commission in performance of its functions.

Data protection commission (DPC)

The DPC is the national independent authority in Ireland responsible for monitoring the application of the GDPR, and is located at 21 Fitzwilliam Square South, Dublin 2. It currently consists of one Data Commissioner and seven Deputy Commissioners.

Enforcements and sanctions

The DPC examines complaints from individuals in relation to potential infringements of data protection law. Where the DPC considers there to be a reasonable likelihood that a complaint can be resolved amicably by the parties, it may take steps it considers appropriate to arrange or facilitate an amicable resolution. In 2020, 4,660 complaints under the GDPR were received by the DPC.

The DPC may conduct a complaints-based statutory inquiry, or a statutory inquiry on its own volition, in order to establish whether an infringement of the GDPR or the DPA 2018 has occurred or is taking place. At 31 December 2020, the DPC had 83 statutory inquiries on hand, comprising 56 domestic inquiries and 27 cross-border inquiries.

> “
>
> THE DPC ISSUED ITS FIRST FINE IN A CROSS-BORDER CASE IN DECEMBER 2020, FINING TWITTER INTERNATIONAL COMPANY 450,000 €.
>
> Patricia McGovern
> *DFMG Solicitors*

The DPC may exercise a broad range of investigatory powers enabling it to gather relevant information and materials (e.g., powers of entry, search and inspection; powers to remove and retain documents and records and to require information and assistance to be provided in respect of an investigation). Where it identifies an urgent need to protect data subjects' rights and freedoms, the DPC can make an ex-parte application to the High Court for an order to suspend, restrict, or prohibit the processing of personal data, or the transfer of the same to a third country or to an international organisation. The DPC may also require a controller or processor to provide a report on a matter specified by it.

The DPC may also impose administrative fines. The DPA 2018 sets the maximum amount of administrative fine on a controller or a processor that is a public authority or public body at 1 million euros, as opposed to the generally applicable maximum of 20 million euros or 4% of annual worldwide turnover in the GDPR. In December 2020, the DPC issued its first fine in a cross-border case, fining Twitter International Company 450,000 €.

DPO

The DPA 2018 does not vary the requirements for the appointment of a DPO, nor has it amended, or added to the role and tasks of the DPO. The DPC has however issued guidelines on the considerations controllers should take into account when assessing the level of knowledge and qualification which they need to ensure their DPO possesses.

Patricia McGovern
DFMG Solicitors

GDPR enforcement in Italy

Further to the entry into force of GDPR, the Data Protection Code (legislative decree no. 196/2003) has been deeply amended by the legislative decree 101/2018, adopted in September 2018 with the aim of integrating and harmonizing to GDPR the previous national regulation.

The Supervisory Authority (Garante per le protezione dei dati personali) worked on several levels and through various channels to provide clarifications on the innovations brought by the new regulation, also following up the on the requests made by entities and trade associations, underling as far as possible that the transition from the previous legal framework to the new one has been seamless.

From a general perspective, 2019 has been, for all stakeholders, a year of stepwise adjustments. Starting from 2020 entities have become increasingly aware of the principles on which GDPR is based (notably the accountability principle) and of the obligations arising from the new regulation and GDPR enforcement has become more effective.

1. The national derogations from GDPR

GDPR requires Member States to legislate in some areas and provides them with the right to integrate the GDPR in others. In this frame, the main derogations from or integration of the GDPR contained in the Data Protection Code, as amended by legislative decree 101/2018, are the following:

- with reference to child's consent, the processing of personal data of a child in relation to information society services is lawful where the child is aged above 14 years (article 2-quinquies);

- the processing of genetic data, biometric data and data relating of health is subject not only to the conditions mentioned in article 9, paragraph 2, GDPR, but also to the safeguards provided by a specific decision issued by the Supervisory Authority every two years (article 2-septies);

- the processing of personal data relating to criminal convictions and offences is allowed only if expressly authorized by a law providing appropriate safeguards for the rights and freedoms of data subjects. Among others, the processing is lawful if authorized by a law concerning: the fulfillment of obligation and exercise of rights by the controller or data subject in the field of labor law or within the framework of employer-employee relationship; establishing, exercising or defending a legal claim; the fulfillment of the obligations set out in the applicable legislation concerning prevention of the use of the 2 financial system for the purpose of laundering the proceeds of crime and financing terrorism (article 2-octies);

- the rights referred to in articles 15 to 22 GDPR may not be exercised if the exercise of those rights may prove factually, effectively detrimental to certain activities such as: the interests safeguarded by anti-money laundering provisions; exercise of a legal claim; confidentiality regarding the identity of the whistleblowers (article 2-undecies);

- criminal fines are provided in case of unlawful data processing due to breach of few provisions of the Data Protection Code (articles 167, 167-bis, 167- ter, 168).

Pursuant to article 2-quarter, the Supervisory Authority has adopted rules of conduct for certain categories of processing of personal data, which contain specific guidelines in the area of processing carried out by journalist, for statistical or scientific research purposes, for historical research purposes and to assert or defend a right in court. Such rules of conduct are part of Annex A of the Data Protection Code.

> “
>
> 2019 HAS BEEN, FOR ALL STAKEHOLDERS, A YEAR OF STEPWISE ADJUSTMENTS.

2. The Supervisory Authority: inspection activity

In the framework of the inspection powers of the supervisory authorities provided for by article 58 GDPR, the Supervisory Authority has the power to order the data controller and the data processor to provide any information it requires for the performance of its tasks and to obtain access to all personal data ant to all information necessary, also related to the contents of databases.

The investigation activities are carried out by the Supervisory Authority together with the Special Data Protection Unit of the Financial Police and are based on an inspection plan, issued by the same Authority every six months.

According to the latest plan, during the first semester of 2021 the inspection activities are aimed, among others, at processing of biometric data for facial recognition including by means of video surveillance systems, processing of personal data carried out by data brokers, by food delivery companies and processing related to data breaches.

Furthermore, the investigation activities are conducted by the Supervisory Authority pursuant to complaints lodged by data subjects according to article 77 GDPR or reports presented by data subjects or by the Financial Police as well as on data breaches.

Marta Margiocco
Cocuzza & Associati Studio Legale

GDPR enforcement in Poland

National Legislation

The Personal Data Protection Act of 10 May 2018 (« Personal Data Protection Act ») entered into force on 25 May 2018 to help implement the GDPR in Poland. The old Personal Data Protection Act of 29 August 1997 has been repealed. Text of the PDPA is available here (in English).

In addition, Act of 21 February 2019 Amending Sectoral Laws to Ensure Application of GDPR (« Amending Act ») aims at adjusting the Polish legal system to the requirements under the GDPR. It introduced changes to almost 170 separate sectoral acts, including Labour Code, Banking Law, Act on Investment Funds and Management of Alternative Investment Funds, Act on the Provision of Electronic Services, Tax Code, Act on Insurance and Reinsurance Activities etc.

The Act of 14 December 2018 on the Protection of Personal Data Processed in Connection with the Prevention and Combating of Crime should also be mentioned. Contrary to the above-mentioned provisions, the enactment of this act was not intended to implement the provisions of the GDPR, but to establish a legal regime for data processing in an area that was excluded from the provisions of the GDPR, i.e. in the field of preventing and combating crime.

Polish Data Protection Authority

The Personal Data Protection Act appointed a new supervisory authority in Poland, namely the President of the Office of Personal Data Protection (« Prezes Urz du Ochrony Danych osobowych » - **PUODO**).
President of the Office of Personal Data Protection
ul. Stawki 2, 00-193 Warsaw
https://uodo.gov.pl/

The following are the most prominent guidelines that have been issued by PUODO:

- list of types of processing activities for which carrying out a Data Protection Impact Assessment (« DPIA ») is required (available in English here)
- guidelines on how to notify PUODO of data breach (available in English here)
- guidelines on how to maintain records with templates for record of processing activities and record of all categories of processing activities and a sample of a completed template (only available in Polish here)
- guidelines on prior consultation (available in English here)
- guidelines on designation of DPO (available in English here)
- guidelines on CCTV (only available in Polish here)
- guidelines on data protection in the workplace (only available in Polish here)
- guidelines on processing personal data in schools and educational establishments (only available in Polish here)
- guidelines on controllers' obligations related to data breaches (available in English here).

National derogations from and additions to GDPR

The most relevant derogations from and additions to the GDPR in the Polish legislation are:

- **Exclusion or limitation of the application of certain provisions of the GDPR.** Personal Data Protection Act excludes the application of the GDPR in several fields. Fully exempt are the activities of special forces as well as the processing of personal data by entities of the public finance sector if such processing is necessary for the execution of tasks which are aimed to ensure the national security.

The PDPA provides that same provisions of the GDPR will not apply where personal data is processed for journalistic purposes, artistic or literary expression (the following articles of the GDPR will not apply: 5-9, 11, 13-16, 18-22, 27, 28 (2)-(10), 30) or for academic purposes (the following articles of the GDPR will not apply: 13, 15 (3)-(4), 18, 27, 28 (2)- (10), 30), e.g. there is an exemption to the obligation to provide privacy notices.
Data controllers conducting public services are exempted from complying with certain obligations to provide privacy notices and respond to subject access requests where it is related to performance of public duties and exercising of these provisions may breach the protection of classified information or prevent or significantly obstruct the proper execution of a public service.

- **Professional secrecy.** The PUODO's right of access to information and personal data is limited by professional secrecy.
The PUODO, and employees of the Office, will be obliged to maintain the secrecy of information that has come to their knowledge in connection with the exercise of their official duties.

- **Employment.** Employers are obliged to request an exhaustive list of data categories from job candidates and employees as set out in the Labour Code; if they want to collect more data directly from job candidates and employees, then consent is required, unless there is a special provision of law that entities can process such data (e.g. criminal convictions of management board members).
However, the processing of a candidate/employee's special categories of personal data by a (potential) employer on the basis of his/her explicit consent is not permitted unless such data is provided t the candidate's/employee's initiative. It is also prohibited in all circumstances for a (potential) employer to process a candidate's/employee's personal data relating to criminal convictions and offences even if such processing is based on his/her consent. The only basis for such processing is a legal obligation.
An employer may (i) use CCTV for the purpose of ensuring employees' security, protecting the employer's property, production control, and

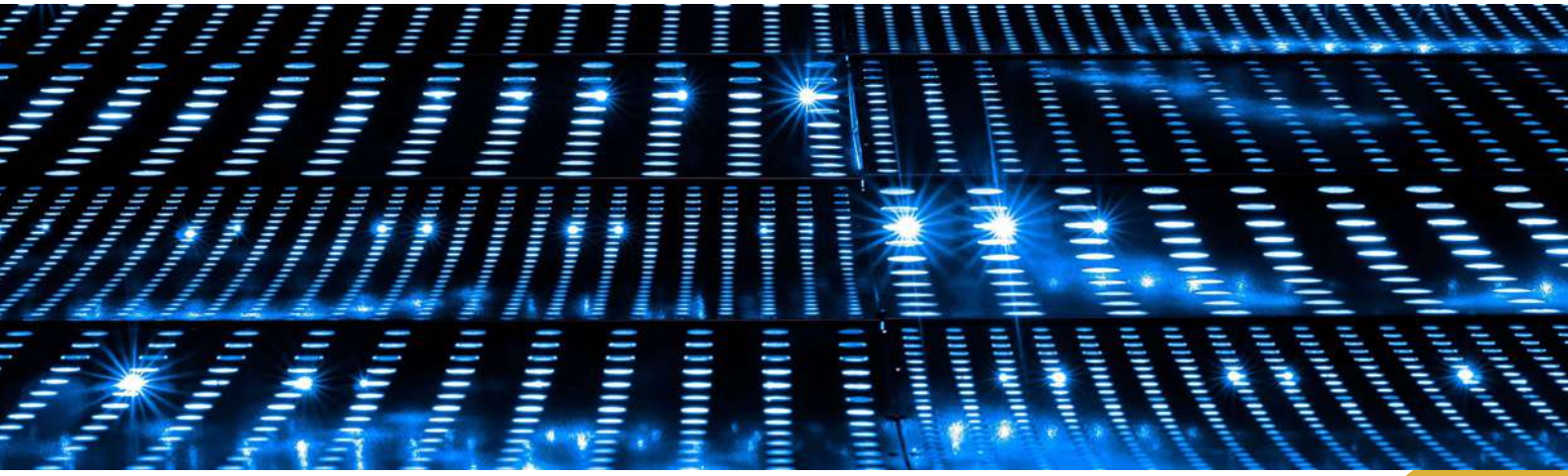
information security; and (ii) monitor employees' emails and use other monitoring methods for the purpose of ensuring that emails are appropriate for the work organization and that employees are making full use of their working hours and appropriate use of the working tools made available to them. The Labour Code sets out more specific rules on employees' monitoring, r.g. it is strictly prohibited to monitor the premises entrusted to trade union organisations, sanitary rooms, cloakrooms, canteens and smoking rooms, unless the monitoring in these rooms is necessary to ensure the safety of employees, the security of the property, the production control, or to keep the confidentiality of the information, disclosure of which could expose the employer to harm.

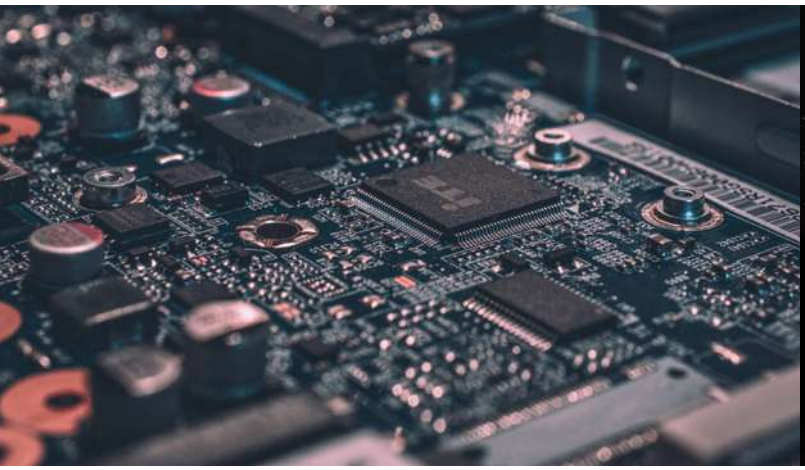
• **Privacy notices.** In Poland, the obligation to provide information to data subject in Polish does not result from Personal Data Protection Act. However, pursuant to the Act on Polish Language any communication with the consumers must be in Polish, so any privacy notices directed at consumers must be in Polish. The same applies to employment relationships.

• **Notice of breach laws.** Pursuant to the Personal Data Protection Act PUODO may introduce an online system enabling controllers to report personal data breaches. PUODO has created such system which enables notification of personal data breach in electronic form. More information on the data breach notification procedure can be found here (in English).

• **Enforcement.** Criminal sanctions for: (i) unpermitted and unauthorized processing, (ii) jeopardizing or impeding a UODO inspection, (iii) failure to provide PUODO with data necessary to determine the basis for an administrative fine. The Personal Data Protection Act also provides that persons who process personal data unlawfully or without authorisation face a criminal fine, restriction of personal liberty or imprisonment of up to two years(-three years if such processing concerns special categories of data). A criminal fine, restriction of personal liberty or imprisonment of up to two years may also be imposed as a criminal sanction for hindering inspection proceedings. Additionally, the Amending Act introduced changes to the Criminal Code that penalize the threat of causing criminal proceedings or other proceedings in which an administrative pecuniary penalty may be imposed. This change is aimed at counteracting GDPR fraud.
The Personal Data Protection Act lowers the level of these administrative fines for public authorities. The fines for public authorities cannot exceed 100,000 PLN (approximately 22,000 €).

• **Special rules for special categories of data.** Changes applicable to the private sector include, e.g., changes to (i) the Act on Insurance and Reinsurance Activity, enabling insurance companies to process personal data, including health data, in an automated manner, including through profiling, in order to assess insurance risk and perform insurance contracts; (ii) the Public Procurement Law, which provides that the transparency principle is not applicable to special categories of personal data collected in a procurement procedure; and (iii) the Banking Law, prohibiting banks from using special categories of data to make decisions based solely on automated processing, including the profiling of personal data in order to access creditworthiness and analyse credit risk.





• **Biometric, genetic or health data.** Employers are allowed to process employees' biometric data where necessary to ensure control over access to particularly important information or to premises requiring special protection. Moreover, a person who will be processing special categories of employees' personal data should be granted a written authorization to do so, and must be obligated to maintain confidentiality.

• **Designation of a Data Protection Officer.** The Amending Act introduces the institution of a deputy DPO, who can act in the absence of the DPO. The same notification requirements apply when designating a deputy DPO. If a group level DPO is appointed and the DPO function is meant to cover Poland as well, then the global DPO must be notified to the UODO. Additionally, a company that designates a DPO is obliged to publish the DPO's contact details, including their name, surname, email address or phone number on its website or, in the absence of a website, in a manner generally accessible at its place of business.

Audits and sanctions

The PUODO carries out audits in accordance with its annual audit plans and outside the scope of its audit plan. The PUODO has not issued the audit plan for 2021 yet, but it will be prepared once the pandemic is contained.

So far, the PUODO has issued several dozen decisions involving administrative fines for various types of non-compliance with the GDPR, such as:

- data breaches that resulted in data leakage;
- lack of cooperation with the PUODO;

> THE HIGHEST FINE IMPOSED BY PUODO WAS 660,000 €

- insufficient fulfilment of data breach notification obligations;
- insufficient legal basis for data processing;
- not providing information required under Article 14 of the GDPR;
- failure to provide a mechanism for withdrawal of consent;
- the absence of an agreement with a data processor and failure to update the register of processing activities;
- other related violations of personal data protection principles.

The total value of the fines imposed is almost two million euros. The highest fine imposed by PUODO was 660,000 € in the case concerning insufficient technical and organisational measures to ensure information security. In seven cases, PUODO decided to issue only a warning.

Babiaczyk Skrocki i Wspólnicy sp.k. provide wide range of services in the cope of GDPR compliance. We develop and review all types of compliance documentation as well as advise our clients on business matters that involve the processing of personal data and specific processing activities. We also offer DPO services.

Dr. Michał Matuszczak
Babiaczyk Skrocki i Wspólnicy sp.k.

GDPR enforcement in the Slovak Republic

In the Slovak Republic the GDPR, its implementation and its enforcement, was a significant topic few years ago, but the initial difficulties and concerns were overcome.

National data protection legislation and derogations from the GDPR

The Slovak Personal Data Protection Act mainly regulates processing of personal data related to the activities of the controller, which do not fall within the scope of EU law, mainly questions regarding personal data processed by the public sector or in the public interest (police force, financial administration etc.). On the other hand, the Slovak Personal Data Protection Act provides several specifications with impact on personal data processing in the private sector:

- The controller may process personal data without consent of the data subject where this processing is necessary for the academic purpose, artistic purpose or literary purpose (subject to further conditions).
- The controller may process personal data without consent of the data subject where this processing is necessary to inform the public by mass media means and where the personal data are processed by a controller based on its field of activity (subject to further conditions).
- The controller that is an employer is allowed to make available or make public personal data of an employee to some extent where necessary in connection with fulfilment of the tasks within the employee employment, service job, or function (subject to further conditions).
- If the data subject dies, the consent requested by the law may be given by a close person to him or her.

Data protection authority

The data protection authority under GDPR in the Slovak Republic is the Office for Personal Data Protection (DPA) with seat at Hranicná 12, 820 07 Bratislava, Slovak Republic which does not have any local branches.

Sanctions and controls

Inspections are carried out by the DPA a) based on its annual plan made by the DPA in advance with the aim of cross-sectional inspections or b) upon complaints or communications about personal data law breaches delivered to the DPA. After 24.05.2018 until 31.12.2019, the DPA started 51 inspections.

Unless planned in advance, inspections and proceedings are started by the DPA upon a complaint by a data subject, that the law was breached. Collective actions or complaints made in favour of data subjects by associations are not allowed. The DPA evaluates the information provided by the complainant and in case of less severe breaches, the DPA sends a so-called communication regarding a potential breach of data protection law to the controller.

In case of more severe or undisputable breaches or if the controller takes no satisfactory remedial action

by himself, the DPA starts official administrative proceedings, carries out an investigation and inspects the controller. Except in cases of obvious, grave breaches of data protection law, inspections are generally concluded by the statement that the breach was remedied during the inspection or that remedial action was officially imposed, which was performed by the controller later. Only a small portion of inspections are typically concluded by a fine - on average in the amount 3489 €. The highest fine imposed so far was around 50.000 €.

DPO

In practice, this kind of services is provided by a wide spectrum of subjects. There are no additional rules or guidelines nor any professional chamber. Law firms usually provide DPO services not directly, but via an affiliated company due to the fact that standard professional insurance of law firms does not cover the activities of a DPO and due to potential conflicts of interests.

Juraj Lukacka
UEPA Advokáti s.r.o.

GDPR enforcement in Spain

National Data Protection legislation and derogations from the GDPR

The Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (« LOPDGDD ») implements the GDPR in Spain and it entered into force on 7th December 2018. Spain has made some considerable derogations from the GDPR, which should definitely be taken into account:

• **Sensitive Personal Data.** Art. 9 (1) Organic Law 3/2018 states that the prohibition of processing special personal data cannot be lifted by the data subject's consent if the main processing purpose is to identify the ideology, trade union membership, religious or philosophical beliefs, sexual orientation or racial/ethnic origin. Art. 9 (2) Organic Law 3/2018 outlines that the following exceptions in Art. 9 (2) lit. e), g), h), i) of the GDPR:

- processing related to personal data that are manifestly made public by the data subject,
- processing necessary for reasons of substantial public interest,
- processing necessary for the purposes of preventive or occupational medicine, for the assessment of an employee's working capacity, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to a contract with a health professional, or
- processing necessary for reasons of public interest in the area of public health

Shall only apply if they are supported by national legislation with the level/rank of « ley » (law). That legislation must make additional requirements to safeguard the security and confidentiality of these special data.

• **Business Contact Data.** There is a presumption that the processing of personal data of business contacts, where the sole purpose is to establish a relationship with the business, will be in the legitimate interests of the controller.

• **Data Protection Officers.** A list of entities that must appoint a data protection officer are set out in the LOPDGDD. This includes, for example, insurers, investment service companies and providers of information society services. Organisations have ten days from the date of appointment of a data protection officer, to notify the Spanish data protection authority of the appointment.

> “
>
> SPAIN HAS MADE SOME CONSIDERABLE DEROGATIONS FROM THE GDPR.
>
> Antonio Muñoz de Gispert & Fanny Porras Delgado-Ureña
>
> *Absis Legal*

• **Children's Data.** Only children aged 14 or over are able to provide valid consent with regard to the receipt of online services.

• **Accuracy of Data.** Article 5(1)(d) of the GDPR requires that personal data be accurate and where necessary kept up to date. The LOPDGDD provides that a controller will not be responsible for processing inaccurate personal data in certain limited circumstances, including where the data were obtained from a public register or the data were received from a third party as a result of a request for data portability.

• **Digital Rights.** The LOPDGDD introduces a number of new digital rights for individuals which go beyond those provided in the GDPR, e.g. the right to privacy and use of digital devices in the workplace. This includes a right to « digital disconnection » that applies to both public and private sector workers. The precise details of how those rights of disconnection will be exercised is generally left to the internal policies of employers as well as collective bargaining processes.

National Data Protection legislation and derogations from the GDPR

The Spanish competent national supervisory authority is the Agencia Española de Protección de Datos (« **AEPD** »), which also represents Spain on the European Data Protection Board. We can provide the contact details of the AEPD if needed.

Tasks and powers of Spanish supervisory authority
The AEPD has enforcement powers and is connected to the Spanish government via the Ministry of Justice. It acts as Spain's representative in the European Data Protection Board. Its task is to supervise the correct application of the GDPR and Organic Law 3/2018.

Sanctions and controls

In the event of a possible violation of regulations or failure to exercise rights, the Inspection Department within the Data Protection Agency analyses the evidence, investigate actions and, when appropriate, instruct the sanctioning procedures. All proposals from the Inspection Department must be approved and signed off by the Director of the Agency.

Complaints can be made directly to the Agency, which is the most frequent situation, although they can also come through a Control Authority of other State members of the European Economic Area (EEA).

The following table shows the number of claims that have entered in the AEPD by each of the different ways of entry.

ENTRIES	2019	2020
CLAIMS SUBMITTED TO THE AEPD	11,590	10,324
CROSS-BORDER CASES FROM THE EEA	790	784
OWN INITIATIVE OF THE AEPD	15	26
NOTIFICACIONS OF SECURITY BREACHES	79	81
TOTAL	12,474	11,215

Source: https://www.aepd.es/es/documento/memoria-aepd-2020.pdf

According to a study recently published by « Finbold », Spain is at the top of the EU members when considering the number of sanctions imposed due to non-compliance with the General Data Protection Regulation in 2020. In 2020 Spain imposed 167 fines for a total amount of 8,018,800 €. The year ended with the imposition of a millionaire fine (five million euros) to a bank. The AEPD estimated minor and very serious infringements of articles 6, 13 and 14 of the RGPD.

According to the AEPD Annual Report for 2020 the areas of activity with the largest numbers of sanctioning procedures concluded in 2020 have been video surveillance (24%), internet services (19%), Public Administrations (10%) and telecommunications (7%).

According to the AEPD Annual Report for 2020 the areas of activity that have been fined the most are financial entities / creditors (63%), telecommunications (13%), fraudulent contracting (7%), debt claims (3%), internet services (3%) and default files (5%).

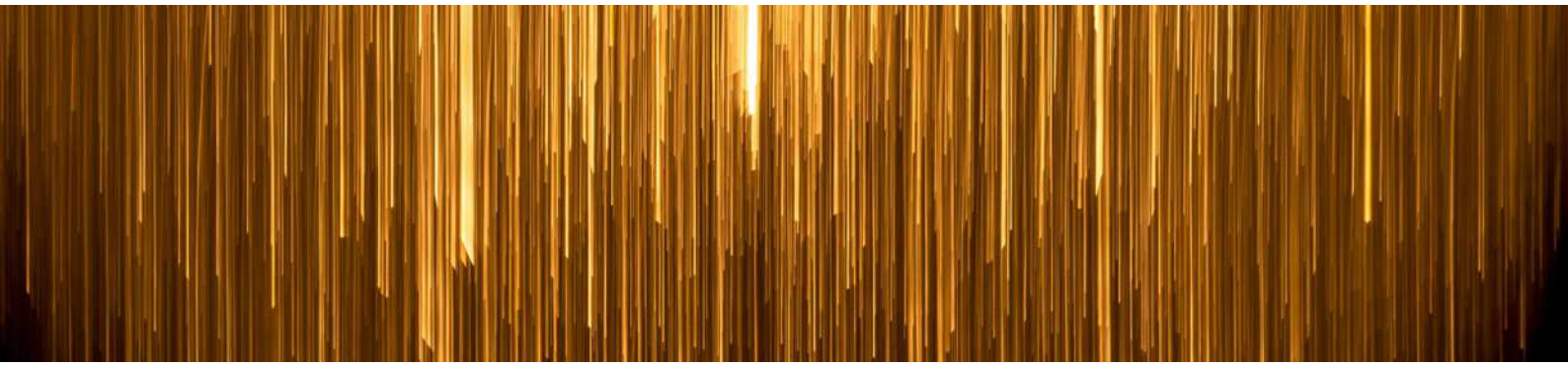
Sanctions related to cookies are expected to see a significant increase in the near future as a result of the adoption of the new criteria stablished by the European Data Protection Board (EDPB).

Regarding the notifications of data breach made to the Agency, these are initially received by the Technological Innovation Division (DIT), which carries out a first analysis. The DIT has received and analysed 1,370 notifications of data breach in 2020, of which only 6% (81) have been referred to the Inspection Department, requiring an in-depth investigation.

DPO

The Spanish law includes a long list of organisations and companies that are required to appoint a DPO. Insurance or reinsurance companies, financial credit institutions, educational institutions, electric and natural gas distributors and advertising and marketing companies, amongst others, are required to appoint a DPO. The LOPD also allows organisations and companies to voluntarily appoint a DPO. Please note that, in either case, the appointment of the DPO must be communicated to the AEPD.

Antonio Muñoz de Gispert &
Fanny Porras Delgado-Ureña
Absis Legal



GDPR enforcement in Sweden

National legislation - derogations and supplements

Sweden is a member of the European Union and therefore subject to the General Data Protection Regulation (Regulation (EU) 2016/679) (the « GDPR »). The GDPR leaves some room for Member States to deviate from and/or supplement the GDPR by means of national legislation; a benefit utilised by Sweden. In addition to the GDPR, the key data protection legislation in Sweden is the Act with Supplementary Provisions to the GDPR (SFS 2018:218) (the « Act ») (an unofficial English version of the Act is available here) and the Ordinance with Supplementary Provisions to the GDPR (SFS 2018:219) (the « Ordinance ») (an unofficial English version of the Ordinance is available here).

The Act and the Ordinance entered into force on 25 May 2018 and replaced the previous Swedish Data Protection Act (SFS 2008:204) and the previous Data Protection Ordinance (SFS 1998:1191).

Among other things, the Act includes provisions on the definition of a child (a data subject at least thirteen (13) years old), when personal identity number(s) may be processed (with consent or if the processing is clearly justified in light of the purpose of the processing, the importance of accurate identification, or on other significant grounds) and that any fines resulting from an infringement should be payed to the state.

Although the Act and the Ordinance supplement the GDPR, they are subsidiary to other specific laws and regulations. Hence, provisions in special laws that deviate from what is stated in the Act or the Ordinance prevail, provided that the special law complies with the GDPR and concerns a matter that may be separately regulated or specified in national law.

In addition, further conditions for the processing of personal data may be found in other laws including:

- The Camera Surveillance Act (SFS: 2018:1200) (only available in Swedish here), which provides conditions for the use of video surveillance and the related processing of personal data;

- The Patient Data Act (SFS (2008:355) (only available in Swedish here), which includes provisions on care providers' processing of patients' personal data (i.e. special categories of personal data); and

- The Criminal Data Act (SFS 2018:1177) (only available in Swedish here), which essentially implements the Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680).

Supervisory authority and enforcement

The ordinance names the Swedish Authority for Privacy Protection (Sw. « Integritetsskyddsmyndigheten » or « IMY »), as the supervisory authority in Sweden.

IMY has a large toolkit of corrective powers available in cases where a controller or processor processes personal data in breach of the GDPR. It may, for example, issue warnings, reprimands, orders (e.g. to bring the processing into compliance with the GDPR), impose a temporary or definitive limitation on the processing operation, withdraw a certification, impose administrative fines and/or suspend certain processing operations. The corrective action chosen should always reflect what is effective and dissuasive in the particular situation, as well as what is proportionate in relation to the nature, gravity, and consequences of the infringement in question.

Issuance of administrative fines is one of many options available to IMY. The amount of the administrative fine will depend on the infringement, the Article to which it relates, and the circumstances in each individual case. IMY will, for example, consider the severity of the infringement, the damage, if the processing included sensitive personal data, and if the infringement was intentional. Historically, the size of the offender has also affected the amount of the fine.

The administrative fine may not exceed 20 million euros or 4% of the group's total worldwide annual turnover, whichever is the highest. For less serious infringements, a maximum fine of 10 million euros or 2% of the group's total worldwide annual turnover will apply, whichever is higher. Swedish authorities risk administrative sanctions amounting to SEK 10 million (approx. 990 000 €), at the most, for Article 83.3 and 83.5 violations and SEK 5 million (approx. 495 000 €), at the most, for Article 83.4 violations.

During 2020, IMY initiated 52 audits and issued decisions in 53. 15 audits resulted in the issuance of administrative fines amounting to SEK 150 million in total. The most noteworthy decisions were (listed chronological with the latest first):

• The Health Care Providers: IMY audited eight health care providers in how they governed and restricted their personnel's access to their main systems for electronic health records. It primarily examined if the health care providers had conducted the needs' and risk analysis required in order to assign adequate access to personal data in the electronic health records. IMY discovered insufficiencies that in seven of the eight cases lead to administrative fines of up to SEK 30 million (fines ranged between SEK 2.5 million to SEK 30 million).

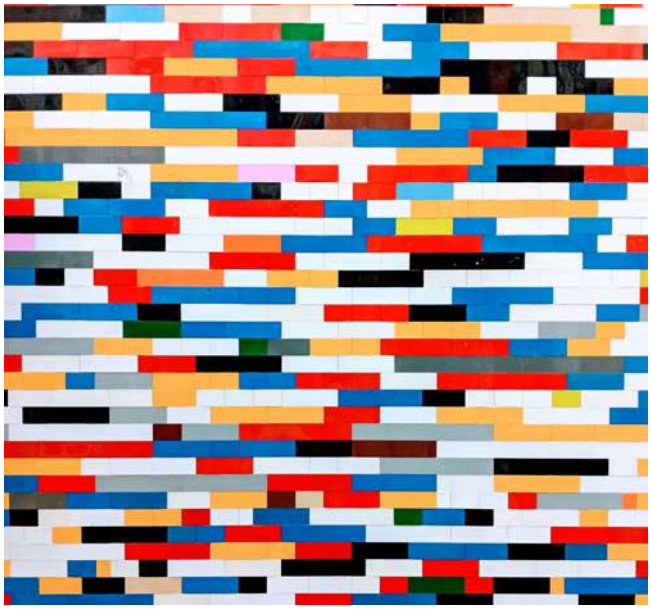
• The School Platform: Following a number of personal data breach notifications, IMY reviewed the IT system used for, among other things, student administration of schools in the city of Stockholm (also known as the « School Platform »). The platform includes personal data of up to 500 000 pupils, guardians and teachers – including classified information and information on protected identity. The review showed an insufficient level of security of such grave nature that IMY issued an administrative fine of SEK 4 million against the Board of Education in the City of Stockholm.

> "
>
> IMY IMPOSED AN ADMINISTRATIVE FINE OF SEK 75 MILLION ON GOOGLE FOR FAILURE TO COMPLY WITH THE GDP.

• The Google Case: IMY imposed an administrative fine of SEK 75 million on Google for failure to comply with the GDPR. IMY found that Google had not fulfilled its obligations in respect of the right to request delisting. The amount was later reduced by the Administrative Court. However, this decision has also been appealed and is to be decided by the Administrative Court of Appeal.

As a result of the Schrems II ruling, IMY has reorganised its supervisory activates and will hereon after consider all complaints received by it – this was not the case pre-Schrems II.

Anna Eidvall & Maria Moberg
MAQS Advokatbyrå



GDPR enforcement in the Netherlands

In the Netherlands, we mostly see the enforcement of the General Data Protection Regulation (GDPR) when there has been a (substantial) data breach in which the safeguards of the GDPR have not or not sufficiently been observed. The supervisory authority also takes action when concrete reports are made. Large scale investigations into compliance with the obligations of the GDPR, without there having been a concrete reason for this, have hardly taken place, or not at all.

Supervisory authority

One of the reasons for this is that our regulator, the so-called « Autoriteit Persoonsgegevens », is facing a major staff shortage. However, the supervisory authority is expected to grow from 184 employees in early 2021 to 470 employees in 2022.

The powers of the supervisory authority are largely described in the GDPR. According to the GDPR, the supervisory authority has the power to fine up to 20 million euro or 4% of the annual turnover (if the latter is higher). However, the GDPR offers room for the member states themselves to allocate additional powers, insofar as this does not impede the cooperation between the supervisory authorities. For instance, according to the Dutch Implementation Act the supervisory authority has the power under certain circumstances to impose an order under administrative coercion or an administrative fine. It is also important that this administrative fine can be imposed on public authorities.

The supervisory authority has imposed 15 fines and 8 orders under administrative coercion since the GDPR came into force. If does not hesitate to impose hefty fines. Recently, a municipality was fined 600,000 € for unauthorised WiFi tracking, a company was fined 725,000 € for the unauthorised use of fingerprints (biometrics) for employee attendance registration and the Credit Registration Office was fined 880,000 € for creating too high thresholds for the right of access.

Although not set in stone, the following steps are taken by the supervisory authority in an investigation:

- Investigation: in this phase, information is gathered;
- Preliminary findings: the supervisory authority makes a draft report in which the facts, findings and preliminary opinion are described. This draft report will be sent to the alleged offender;
- Opinion: the alleged offender will have 2 to 4 weeks to respond to the preliminary findings verbally or in writing;
- Final findings: the supervisory authority sends the alleged offender the final investigation report.

• Publication: Investigation reports are published.

• Enforcement: The supervisory authority can use its enforcement powers.

There is a possibility to object and appeal the decision of the supervisory authority.

Deviations GDPR in Implementation Act

The Implementation Act further fills in the room that the GDPR leaves to the member states in certain areas. The Implementation Act regulates, among other things, the following:

• the tasks and powers of the supervisory authority;

• the exceptions that apply in the Netherlands to the ban on processing categories of special personal data;

• the provisions on legal protection;

• the data protection officer's duty of confidentiality;

• the other exceptions and limitations in relation to the GDPR.

Special personal data

The Implementation Act provides some exceptions to the ban on processing special categories of personal data. These include the following exceptions:

• processing of special categories of personal data on the basis of a general exception, such as the explicit consent of the data subject or for the protection of the vital interests of the data subject or of another person;

• processing of personal data revealing racial or ethnic origin when this is necessary to identify the data subject;

• processing of biometric data when this is necessary for authentication or security purposes;

• processing of data concerning health by care providers, health institutions or social services, when this is necessary for the proper treatment or care of the person concerned, also in an employment relationship.

Other exceptions

The Implementation Act also mentions, among other things, the following exceptions and limitations:

• Automated individual decision-making is permissible if it is necessary in order to comply with a legal obligation or if it is necessary for the fulfilment of a task in the public interest (with the exception of profiling);

• The GDPR and the Implementation Act partly do not apply to the processing of personal data for exclusively journalistic purposes and for the purpose of academic, artistic or literary expression;

• A national identification number may only be used in the processing of personal data for the purposes of implementing the relevant law or for purposes specified by law.

The Implementation Act is up for revision, but no major changes are expected.

Natascha Niewold
Valegis Advocaten

DATA, INFORMATION & CYBER LAW

Members & Contacts

Theresa Adamek
klein • wenner
44, avenue des Champs-Elysées, 75008 Paris, France
T: +33 1 44 95 20 00
E: theresa.adamek@kleinwenner.eu

Laurent Badiane
klein • wenner
44, avenue des Champs-Elysées, 75008 Paris, France
T: +33 1 44 95 20 00
M: +33 7 88 18 01 25
E: laurent.badiane@kleinwenner.eu

Nikolay Belokonski
KWR Belokonski Gospodinov & Partners
Alexander Zendov str. 1, fl.6, Nr.38, Sofia 1113, Bulgaria
T: +359 2 971 55 32
M: +359 887 40 94 95
E: nikolay.belokonski@kwrbg.eu

Julia Bhend
Probst Partner AG
Bahnhofplatz 18, CH-8401 Winterthur, Switzerland
T: +41 52 269 14 00
E: julia.bhend@probstpartner.ch

Matthieu Bourgeois
klein • wenner
44, avenue des Champs Elysées, 75008 Paris, France
T: +33 1 44 95 20 00
M: +33 6 64 41 63 27
E: matthieu.bourgeois@kleinwenner.eu

Barbara Kuchar
KWR Karasek Wietrzyk Rechtsanwälte GmbH
Fleischmarkt 1, 3 rd floor, A-1010 Vienna, Austria
T: 43 1 24 500 3145
E: barbara.kuchar@kwr.at

Isaac D. López
Cayad - Cancino Ayuso Abogados
Mexico city, Mexico
T: 52 20 01 01, ext. 119
E: ilopez@cayad.com

Marta Margiocco
Cocuzza & Associati Studio Legale
Via San Giovanni Sul Muro 18, 20121 Milano, Italy
T: +39 02-866096
E: mmargiocco@cocuzzaeassociati.it

Michał Matuszczak
Babiaczyk, Skrocki i Wspólnicy Sp. K
ul. Wyspianskiego 43, 60 – 751 Poznan, Poland
T: +48 61 8441 733
E: m.matuszczak@bsiw.pl

Patricia McGovern
DFMG Solicitors
Embassy House, Ballsbridge, Dublin D04 H6Y0, Ireland
T: +353 1 637 6600
D: +353 1 637 6614
E: pmcgovern@dfmg.ie

Anna Mertinz
KWR Karasek Wietrzyk Rechtsanwälte GmbH
Fleischmarkt 1, 3 rd floor, A-1010 Vienna, Austria
T: +43 1 24 500 3131
E: anna.mertinz@kwr.at

Sebastian Meyer
BRANDI Rechtsanwälte
Adenauerplatz 1, 33602 Bielefeld, Germany
T: +49 521 96535 812
E: sebastian.meyer(at)brandi.net

Razvan Miutescu
Whiteford, Taylor & Preston
7 St. Paul Street, Baltimore, MD 21202-1636, USA
T: +1 410 347 8744
E: rmiutescu@wtplaw.com

S. Keith Moulsdale
Whiteford, Taylor & Preston
7 St. Paul Street, Baltimore, MD 21202-1636, USA
T: +1 410 347 8721
E: skmoulsdale@wtplaw.com

Tomáš Mudra
UEPA advokáti s.r.o.
Voctárova 2449/5, 180 00 Prague, Czech Republic
T: +420 234 707 444
E: TMU@uepa.cz

Antonio Muñoz de Gispert
Absis Legal
c/ Muntaner 379, Ent. 1º, 08021 Barcelona, Spain
T: +34 93 531 91 00
M: +34 650 41 33 70
E: amunoz@absislegal.com

Tomislav Pedišić
Vukmir & Associates
Gramaca 2L, 10000 Zagreb, Croatia/Hrvatska
T: +385 1 390 0508
E:tomislav.pedisic@vukmir.net

Katharina Windisch
KWR Karasek Wietrzyk Rechtsanwälte GmbH
Fleischmarkt 1, 3 rd floor, A-1010 Vienna, Austria
T: +43 1 24 500 3131
E: katharina.windisch@kwr.at

CONNECT WITH US

PANGEANET
INTERNATIONAL NETWORK OF INDEPENDENT LAW FIRMS

To find our other publications and newsletters

CLICK HERE

Email: info@pangea-net.org
Website: www.pangea-net.org
Linkedin: /company/pangeanet