



SIGN UP

PANGEANET

INTERNATIONAL NETWORK OF INDEPENDANT LAW FIRMS

VISIT OUR WEBSITE

NEWSLETTER 4

May 2022

DATA, INFORMATION & CYBER LAW

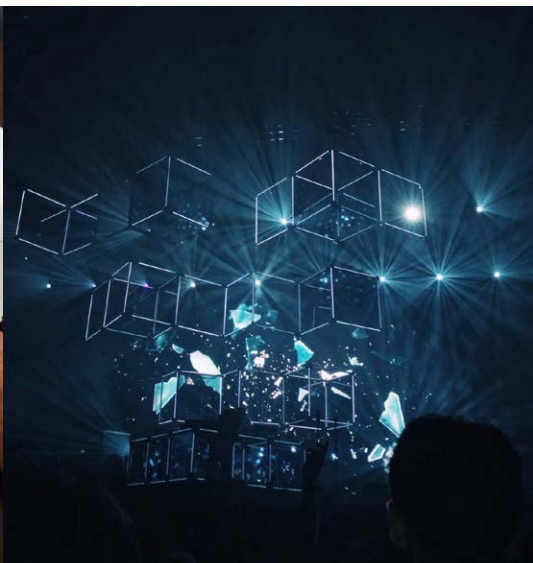
PangeaNet is an association of independent law firms from over 25 countries forming an international law firm network. The Pangea Practice Group for Data, Information and Cyber Law (DICL) consists of experts in IT, data protection law, privacy, cybersecurity and open data issues. We support your digital 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



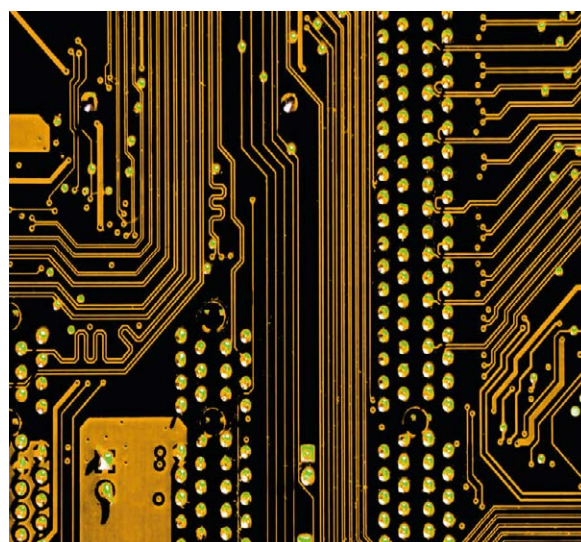
4 YEARS LATER : AN ANALYSIS OF GDPR ENFORCEMENT AND WORLDWIDE IMPACT

Important topics of the fourth anniversary of the GDPR. The 25 May 2022 marks the fourth anniversary of the European General Data Protection Regulation (GDPR) coming into force. In this newsletter, the Pangea DICL team reflects on key trends across 10 of jurisdictions (Poland, Ireland, Switzerland, Italy, Bulgaria, Czech Republic, Austria, Belgium, Germany and Croatia) in particular looking ahead to issues that are coming into focus (cookies, cloud services, video surveillance and services of facial recognition, etc.).

According to the Pangea DICL team, GDPR awareness and enforcement are on the rise during this fourth year of application of the GDPR. Data subject rights have also been an important topic. The analysis reveals that the right of access, the right to be forgotten and the right to object to direct marketing are the most commonly enforced in all jurisdictions. Rights to obtain information about processing and to withdraw consent also appear to be more subject to enforcement. The number of fines issued under the GDPR has increased across the board. The record amount of fines remains held by Ireland's Data Protection Commission, which imposed a €25 million fine on WhatsApp in September 2021.

New Standard Contractual Clauses under GDPR.

In terms of data transfers, the fourth year of the GDPR is likely to be as interesting as the third year. On 4 June 2021, the European Commission issued modernised standard contractual clauses under the GDPR for data transfers. These modernised SCCs replace the two sets of SCCs that were adopted under the previous Data Protection Directive 95/46. Since 27 September 2021, it is no longer possible to conclude contracts incorporating these earlier sets of SCCs. Until 27 December 2022, controllers and processors can continue to rely on those earlier SCCs for contracts that were concluded before 27 September 2021, provided that the processing operations that are the subject matter of the contract remain unchanged.



GDPR worldwide impact. Since its adoption in 2018, the GDPR has become the benchmark for new data protection legislations around the world. Many countries outside the EU have sought parity with the GDPR in order to obtain a positive adequacy ruling from the European Commission, which would allow a free data flow between their country and the European market. In recent years, legislators' efforts have enhanced, with many data protection law initiatives being passed and adopted. The year 2022 is expected to continue this trend, with regions such as the United States, Europe and the Asia Pacific introducing or amending data privacy and protection laws. For example, on 20 August 2021, China adopted its first data protection legislation, the Personal Information Protection Law (PIPL). It came into effect on 1 November 2021. In 2021, US states of Virginia and Colorado followed in the footsteps of California and also passed data protection laws that will come into force in 2023. In Switzerland, the revised Federal Data Protection Act was passed by the Federal Council in September 2020 and is expected to enter into force in the second half of 2022. However, an official date has not yet been set.

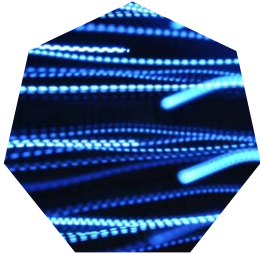
Enjoy your read !



Laurent Badiane & Matthieu Bourgeois
klein • wenger, France

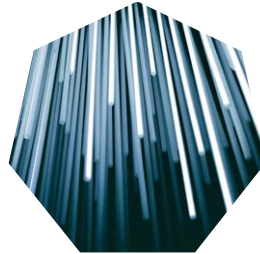


Index



GDPR
in Austria

4



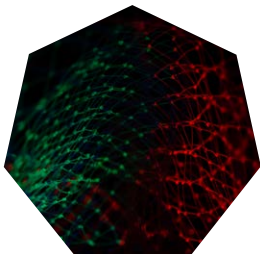
Belgium - The Belgian data
protection authority strikes
the adtech industry

5



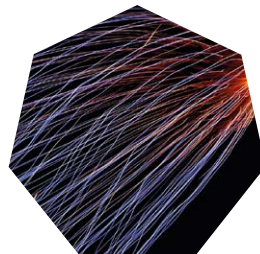
GDPR
in Bulgaria

6



GDPR in the
Republic of Croatia

7



Czech Republic – time
of inconspicuous yet
significant changes

8



GDPR in Germany -
developments over the
past year

8



Ireland - Data Protection
highlights 2021-2022

10



GDPR
in Italy

11



Poland - Constant increase in
legal awareness regarding the
protection of personal data

11



Cloud Services for the
Public Administration
in Switzerland

12

GDPR in Austria

In Austria, the past 12 months have been dominated by high penalties and the Google Analytics decision (D155.027).

1) Updates on the Data Protection Authority and level of compliance

The Austrian Data Protection Authority (DPA) has increased its workforce by 13 employees and set up a « task force » for dealing with complaints regarding cookies and cookie banners. There are no official evaluations of the level of compliance among Austrian companies.

2) Penalties or other sanctions

According to the DPA report of 2021, penalties of almost EUR 25 Mio were imposed (not legally binding yet). This shows that the DPA is imposing very high penalties, also on partly state-owned companies.

“
THE DPA IS IMPOSING
VERY HIGH PENALTIES,
ALSO ON PARTLY STATE-
OWNED COMPANIES

Anna Mertinz & Jennifer Held

*KWR Karasek Wietrzyk
Rechtsanwälte GmbH*

3) Google Analytics

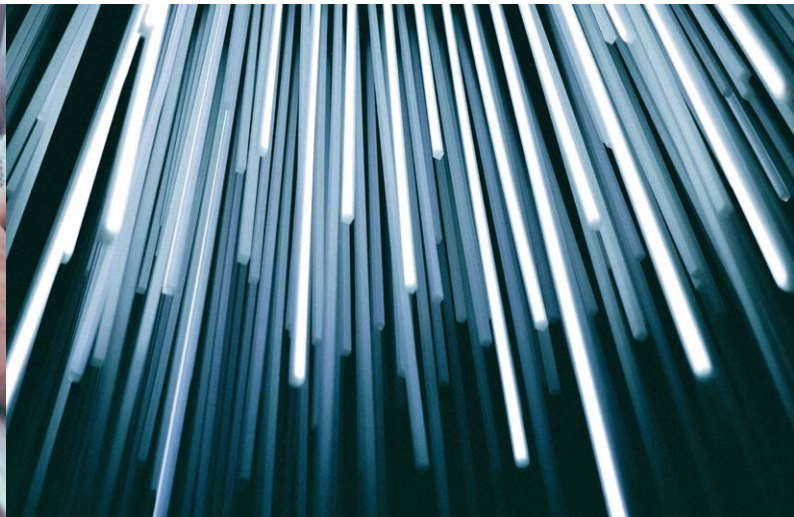
The DPA held that the use of Google Analytics violates the GDPR. Short summary:

- a. When using Google Analytics, personal data is processed.
- b. Standard Contractual Clauses and supplementary measures do not provide the necessary appropriate safeguards for transferring data to the US.



Anna Mertinz & Jennifer Held

KWR Karasek Wietrzyk Rechtsanwälte GmbH



• BELGIUM

Belgium - the Belgian data protection authority strikes the adtech industry: the consent framework of IAB Europe infringes the GDPR

The Belgian DPA has ruled in a decision of 2 February 2022 that the Transparency and Consent Framework (TCF), developed by IAB Europe, does not comply with a number of provisions of the GDPR.

The TCF is a widespread mechanism that facilitates the management of user preferences for online personalised ads, and plays a key role in so-called Real Time Bidding (RTB). The lawfulness of processing personal data in the context of RTB is questioned, so the decision is of particular relevance to the whole online advertisement industry.

The Belgian DPA identified a series of GDPR infringements by IAB Europe:

- there was no legal basis for the different processing activities in the context of RTB;
- the information that was provided to the data subjects was too generic and vague;

- there was a lack of organisational and technical measures in accordance with the principle of data protection by design and by default;

- IAB Europe had also failed to keep a register of processing activities, to appoint a DPO and to conduct a « DPIA » (data protection impact assessment).

The Belgian DPA has imposed a fine of 250.000,00 EUR on IAB Europe and gave the company two months to submit an action plan to bring its operations into compliance. IAB Europe has already announced that an appeal will be lodged.



Michiel Beutels
Litiguard Law Firm



GDPR in Bulgaria

In 2021, the Bulgarian Commission for Personal Data Protection (« CPDP » or « Commission ») has been contacted with over 840 complaints.

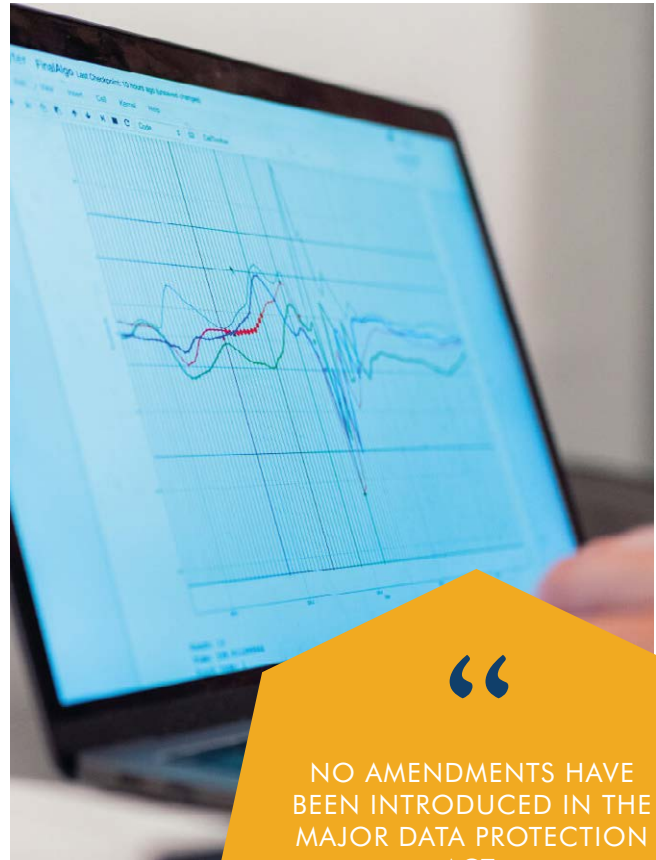
Increased number of complaints against video surveillance – 196, and breaches in the provision of postal and courier services. Total amount of fines is 319 000 BGN, imposed are also warnings, prohibitions and injunctions.

No amendments have been introduced in the major Data Protection Act. However, enhanced practice of the CPDP in accordance with the EDPB's Draft of Guidelines for the implementation of Art. 62 of the GDPR and Guideline 01/2021. Enhanced analysis of artificial intelligence, facial recognition, protection of children's personal data on the internet, big data and the related possibility of its profiling. Enhanced efforts towards full Schengen membership in 2021 - checks on national systems/units of the second generation Schengen Information System (SIS II), the Visa Information System (VIS) and the national consular service.



Nikolay Belokonski

KWR Belokonski Gospodinov & Partners

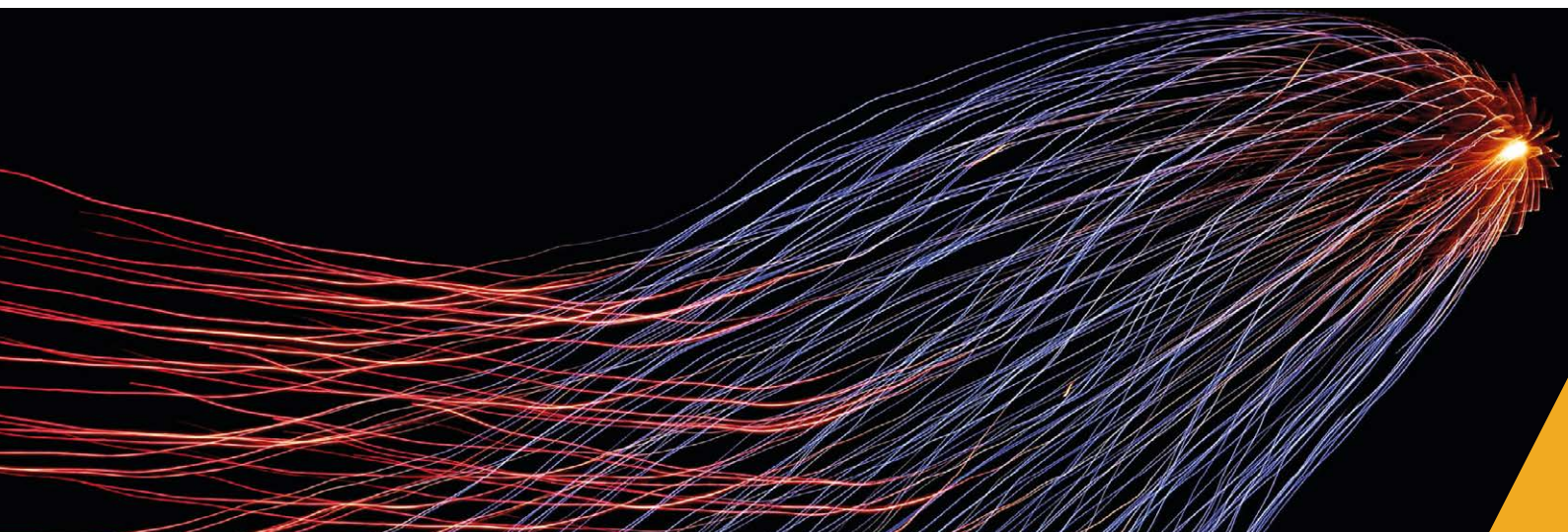


“

NO AMENDMENTS HAVE BEEN INTRODUCED IN THE MAJOR DATA PROTECTION ACT.

Nikolay Belokonski

KWR Belokonski Gospodinov & Partners





GDPR in the Republic of Croatia

The Croatian Data Protection Authority (DPA) recently imposed two administrative fines in total amount of HRK 1,6 million.

Namely, an administrative fine for failing to provide copies of the personal data (video surveillance records) at the request of the data subjects. The fine was imposed in the amount of 940.000,00 HRK (cca EUR 125 000) to the data controller, i.e. a company in the sector of energetics due to the infringement of article 15.3. of the GDPR, violation of the right to access personal data by the data subject. More precisely, upon the specific request of the data subject, the data controller initially refused to provide requested copies on the grounds that it considered there existed no written request in this respect from the competent authorities for providing subject copies, the purpose of the request was not justified and providing copy would, in its opinion have adverse effects on rights of its employees and the customers. Data subject addressed the DPA which expressed its opinion

on mandatory requirement for the controller to issue subject copies to the data subject, following, which data controller responded that the requested copies could not be delivered to the data subject given that copies of their video surveillance records are deleted after seven (7) days.

The DPA determined there existed indirect damage for the data subject and possible financial benefit for the data controller, which by failing to provide requested copies and with deletion thereof eliminated important evidence in the dispute and thus avoided financial damage which it could have suffered in the consumer dispute with the data subject.

Other administrative fine was imposed by DPA for failing to take appropriate security measures for the processing of personal data. The fine was imposed in the amount of 675.000,00 HRK (cca EUR 90.000) to a retail chain as data controller for acting contrary to the article 32.1.b) and d) and 32.2. and 32.4. of GDPR which led to



THE DPA IMPOSED AN ADMINISTRATIVE FINE FOR FAILING TO PROVIDE COPIES OF THE PERSONAL DATA (VIDEO SURVEILLANCE RECORDS) AT THE REQUEST OF THE DATA SUBJECTS, AS WELL AS FOR FALLING TO TAKE APPROPRIATE SECURITY MEASURES FOR THE PROCESSING OF PERSONAL DATA.

unauthorized processing of personal data of data subjects by making them publicly available on social networks and in the media. More precisely, the respective data controller reported to the DPA on internal data breach, i.e. on unauthorized processing of video surveillance records by its employees who made copy of the records by their mobile camera and published the records to social networks and in the media. The DPA found that the data controller did not take appropriate technical and organizational safety measures, neither before nor after the incident, which could have reduced the risk of the same or similar incident to a minimum. Even though the

data controller did have some measures in place, the DPA considered that the data controller did not regularly conduct supervision of the implementation of such technical and organizational measures and failed to regularly examine and evaluate the effectiveness of these measures envisaged for ensuring safety of data processing through video surveillance.



Andrea Kožul Pedišić
Vukmir & Associates



Czech Republic - time of inconspicuous yet significant changes

The Covid-19 pandemic brought upon new challenges regarding personal data and shifted society's focus a lot to the processing of personal data within employment relationships. People are also gradually more concerned about their personal data – the number of complaints also increased. The most common misconducts are having no proper legal title, using data for different purposes than what they were collected for and failing to inform the data subjects about the processing. The highest fine imposed in 2021 was approx. 80.000 EUR.

Cookies and cloud services also getting a lot of attention recently.

The Czech Personal Data Protection Act mainly The Czech Republic finally aligned with the EU-standard and adopted the opt-principle when allowing cookies in browsers, which was not welcomed but due to the availability of international solutions, most addressees have tried to comply. However it remains to be clarified by respective decisions, if some of these solutions are fully in accordance with GDPR. The Czech DPA is aware of that and plans to focus its inspection activities on this field as well.



Tomáš Mudra
UEPA Advokáti s.r.o.



GDPR in Germany - developments over the past year

The abstract-general requirements of the GDPR have been concretized in the past twelve months, among other things, by the statements of the supervisory authorities in Germany; in addition, the statements help with the practical implementation of measures such as those related to the data

protection challenges of the Corona pandemic. However, it is apparent that there are still numerous imponderables for all parties involved, particularly in fine proceedings, and that current fine decisions often do not stand up to judicial review.



Statements from data protection supervisory authorities

A large number of supervisory authority statements concerned the data protection challenges posed by the Corona pandemic. For example, the German Conference of the Independent Federal and State Data Protection Authorities published a statement on contact tracing in times of the Corona pandemic as well as guidance on the use of digital services for contact tracing.

Another topic was the compatibility of fax use with the GDPR, on which both the Hessian Commissioner for Data Protection and Freedom of Information and the State Data Protection Commissioner in Bremen commented. In their view, the transmission of personal data by fax could violate the GDPR in particular if it involves data requiring special protection, for example, special categories of personal data pursuant to Article 9(1) of the GDPR.

Fines imposed by data protection supervisory authorities

Fines imposed by German data protection supervisory authorities last year include, for example, a fine of 10.4 million euros imposed by the Lower Saxony Data Protection Commissioner on [notebooksbilliger.de](https://www.notebooksbilliger.de) AG for video surveillance of employees without a sufficient legal basis. A fine of 900,000 euros was imposed on the energy supplier Vattenfall Europe Sales GmbH by the Hamburg Commissioner for Data Protection and Freedom of Information due to the company's failure to provide data subjects with sufficiently transparent information about an internal data comparison in connection with contract inquiries.

Some companies were able to successfully defend themselves against the fines imposed. In the first instance, the Berlin Regional Court considered a fine imposed by the Berlin data protection supervisory authority against Deutsche Wohnen SE to be ineffective, as in its opinion the company cannot be sanctioned if it cannot be proven that the fault lies with management personnel (Berlin Regional Court, decision dated February 18, 2021, ref. 526 AR). In the second instance, the Court of Appeal in Berlin referred questions on the requirements for setting fines to the European Court of Justice (ECJ) (Court of Appeal, decision dated December 6,

2021, ref. 3 Ws 250/21). Resolving the question of whether the internal responsibilities of a legal entity must be clarified in order to impose a fine, despite the proven existence of a data protection breach, is relevant for the fine practice of all German data protection supervisory authorities. If the answer is in the affirmative, a fine may frequently not be imposed in Germany in those cases – not uncommon among larger companies – in which it is not possible to prove responsibility.

National legislation

The new Telecommunications Telemedia Data Protection Act (TTDSG) came into force in Germany on December 1, 2021, in which the legislature implemented the requirements of the E-Privacy Directive and the case law of the ECJ and the German Federal Court of Justice regarding the use of cookies and similar technologies in a national regulation. The main purpose of the Act is to protect privacy in the use of telemedia and telecommunications services and to protect the secrecy of telecommunications.

The TTDSG applies to all companies and persons who have a branch office, provide services, participate in the provision of services or make goods available on the market within the scope of the TTDSG. The opening of the geographical scope of application of the TTDSG is based on the marketplace principle, which is already standardized in the GDPR. The provisions of the TTDSG are therefore also applicable to providers outside Germany, provided their services are geared to the German market. In addition, the country-of-origin principle standardized in Section 3 of the German Telemedia Act continues to apply to telemedia providers, according to which European service providers established in Germany are subject to the requirements of German law even if the telemedia are offered or distributed on a businesslike basis in another EU country. Both German and non-German providers must therefore check whether the TTDSG, with its special permissions and information requirements, applies to them.



Dr. Sebastian Meyer & Johanna Schmale
BRANDI Rechtsanwälte



Ireland - Data Protection highlights 2021-2022

The most frequent GDPR topics for queries and complaints include access requests, fair-processing, disclosure, direct marketing and the right to be forgotten.

In September 2021 the Data Protection Commission (DPC) announced a conclusion to a GDPR investigation conducted into WhatsApp Ireland Limited. The decision was subject to the EU dispute resolution process, after which the DPC imposed a fine of 225 million EUR on WhatsApp and an order for WhatsApp to bring its processing into compliance. On 15 March 2022 the DPC adopted a decision imposing a fine of 17 million EUR on Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) following an enquiry into a series of 12 data breach notifications.

According to the Commissioner: « It is clear that “data controllers” in Ireland continue to improve their compliance efforts, but higher standards of responsiveness to individuals seeking to exercise their rights are still needed in many sectors. »



Patricia McGovern
DFMG Solicitors



IT IS CLEAR THAT “DATA CONTROLLERS” IN IRELAND CONTINUE TO IMPROVE THEIR COMPLIANCE EFFORTS, BUT HIGHER STANDARDS OF RESPONSIVENESS TO INDIVIDUALS SEEKING TO EXERCISE THEIR RIGHTS ARE STILL NEEDED IN MANY SECTORS.

Patricia McGovern
DFMG Solicitors

GDPR in Italy

With a decision rendered in February 2022, the Italian Supervisory Authority imposed a fine of Eur 20 million to Clearview AI - a US company which offers services of facial recognition based on images extracted via web scraping - due to the unlawful processing of biometric and geolocation data of individuals located in the Italian territory.

The inquiry activities carried out by the Supervisory Authority - which started from press news, a few complaints lodged by data subjects and alerts of data protection associations – pointed out that Clearview AI facial recognition system did allow the tracking of individuals located in Italy. Such tracking was carried out in breach of fundamental

principles of European data protection regulation such as transparency, purpose limitation and storage limitation and without an appropriate legal basis.

In addition to the fine, the Italian Supervisory Authority banned any processing of personal data through the US company facial recognition system and ordered the same to delete the biometric and common data processed related to individuals located in Italy.



Marta Margiocco
Cocuzza & Associati Studio Legale



CLEARVIEW AI FACIAL RECOGNITION SYSTEM DID ALLOW THE TRACKING OF INDIVIDUALS LOCATED IN ITALY.

Constant increase in legal awareness regarding the protection of personal data

A constant trend in Poland is the increase in awareness of the rights and obligations resulting from GDPR. Last year, the Polish supervisory authority received over 8,500 complaints about a breach of data protection. The data controllers reported almost 13,000 cases of violations in the last year.

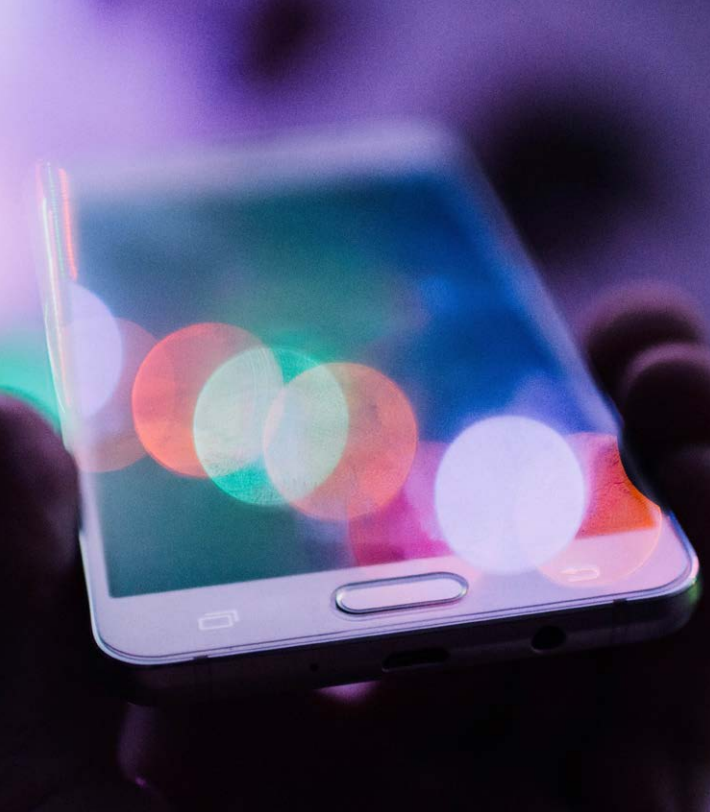
Moreover, the supervisory authority noted a significant increase in the number of legal questions submitted to the office regarding the application of the GDPR. This shows that data controllers, data protection officers and citizens themselves identify problems very quickly and expect guidance.

Since 2018, the supervisory authority has imposed more than 40 fines totaling almost 3.5 million EUR. The problem is that only slightly over 32,000 EUR was actually paid by the punished entities. The convicted entities appeal against the decision to impose a penalty, and time-consuming court procedures delay the execution of the decision. So far, almost all of the completed court cases have been resolved in favor of the supervisory authority.



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

Cloud Services for the Public Administration in Switzerland



While Switzerland is still waiting for the entry into force of the revised Federal Data Protection Act FDPA (recent news announced it for September 2023) and for the publication of the revised Ordinance to the FDPA, companies have already started to implement the new rules. Apart from that, many businesses are in the course of implementing the new Standard Contractual Clauses for data transfers abroad and develop an approach for the data transfer impact assessment (TIA) for data transfers in third countries.

“

THE ZURICH GOVERNMENT APPROVED THE USE OF MICROSOFT 365 FOR THE CANTONAL PUBLIC ADMINISTRATION AND SET A STANDARD METHOD TO ASSESS THE RISK OF LAWFUL ACCESS FOR CLOUD SERVICES.

The data export requirements and TIA are particularly important with respect to cloud services of providers with US headquarters. In this connection, a decision

taken by the government of the Canton of Zurich (the most populous Canton of Switzerland) in March 2022 has been highly discussed.

The Zurich government approved the use of Microsoft 365 for the cantonal public administration and set a standard method to assess the risk of lawful access for cloud services.

Moreover, it decided that if the 90% probability that a lawful access occurs is beyond 100 years, the cantonal public administration is allowed to use the cloud service without further approval. For Microsoft 365, the Zurich government assessed that it will take 1'206 years until one lawful access will occur with a probability of 90% when using Microsoft 365 with the technical and organisation security measures that will be implemented to protect the data in the cloud.



Julia Bhend
Probst Partner AG



DATA, INFORMATION & CYBER LAW

Members & Contacts

Laurent Badiane

klein • wanner

44, avenue des Champs-Élysées, 75008 Paris, France
T: +33 1 44 95 20 00
E: laurent.badiane@kleinwanner.eu

Michał Matuszczak

Babiaczek, Skrocki i Wspólnicy Sp. K

ul. Wyspiańskiego 43, 60 – 751 Poznań, Poland
T: +48 61 8441 733
E: m.matuszczak@bsiw.pl

Antonio Muñoz de Gispert

Absis Legal

c/ Muntaner 379, Ent. 1ª, 08021 Barcelona, Spain
T: +34 93 531 91 00
E: amunoz@absislegal.com

Nikolay Belokonski

KWR Belokonski Gospodinov & Partners

Alexander Zendov str. 1, fl.6, Nr.38, Sofia 1113, Bulgaria
T: +359 2 971 55 32
E: nikolay.belokonski@kwr.bg

Patricia McGovern

DFMG Solicitors

Embassy House, Ballsbridge, Dublin D04 H6Y0, Ireland
T: +353 1 637 6600
E: pmcgovern@dfmg.ie

Richard Nicholas

Browne Jacobson

Victoria Square House, Birmingham, B2 4BU, England
T: +44 1 21 237 3992
E: richard.nicholas@brownejacobson.com

Julia Bhend

Probst Partner AG

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

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

Tomislav Pedišić

Vukmir & Associates

Gramaca 2L, 10000 Zagreb, Croatia/Hrvatska
T: +385 1 390 0508
E: tomlav.pedisic@vukmir.net

Matthieu Bourgeois

klein • wanner

44, avenue des Champs-Élysées, 75008 Paris, France
T: +33 1 44 95 20 00
E: matthieu.bourgeois@kleinwanner.eu

Sebastian Meyer

BRANDI Rechtsanwälte

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

Lauren Webb

Browne Jacobson

Victoria Square House, Birmingham, B2 4BU, England
T: +44 1 21 237 4573
E: lauren.webb@brownejacobson.com

Theresa Castelan

klein • wanner

44, avenue des Champs-Élysées, 75008 Paris, France
T: +33 1 44 95 20 00
E: theresa.castelan@kleinwanner.eu

Razvan Miutescu

Whiteford, Taylor & Preston

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

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

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

S. Keith Moulds

Whiteford, Taylor & Preston

7 St. Paul Street, Baltimore, MD 21202-1636, USA
T: +1 410 347 8721
E: skmoulds@wtplaw.com

Marta Margiocco

Cocuzza & Associati Studio Legale

Via San Giovanni Sul Muro 18, 20121 Milano, Italy
T: +39 02-866096
E: mmargiocco@cocuzzaeassociati.it

Tomáš Mudra

UEPA advokáti s.r.o.

Vocáárova 2449/5, 180 00 Prague, Czech Republic
T: +420 234 707 444
E: TMU@uepa.cz



READ OUR ANNUAL
REPORT 2020/2021

CONNECT WITH US



PANGAANET
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](https://company/pangeanet)