FIDE 2021 Congress - Topic 2: The New EU Data Protection Regime

Brief overview most relevant updates

Table of Contents

General update: Belgium

Written by: Anneleen Van de Meulebroucke

The Impediments to the enforcement of GDPR

The budget that was allocated to the Belgian Data Protection Authority remains rather limited. As a consequence, we notice that there is a delay in the treatment of cases by the Data Protection Authority. Yet, we also notice that an ever increasing number of cases is treated compared to the years before and that caselaw is developing. The caselaw of the Belgian Market Court (Marktenhof/Cour des marchés), which is the appeal instance for decisions of the Data Protection Authority, is also developing, and annulling some of the decisions issued by the Belgian Data Protection Authority, e.g. for a violation of the rights of defence or lack of motivation.

Beyond NSAs: the role of other actors in developing data protection

Several privacy activists are operating in Belgium, such as the Ministry of Privacy (see: https://ministryofprivacy.eu/), and the Liga for Human Rights ("Liga voor Mensenrechten" – see: https://mensenrechten.be/). These brought, among others, the case re the use of digital fingerprints before the constitutional court (see question 4).

Recently, two attorneys acting on behalf of different natural and legal persons headed to the Constitutional Court in the context of the Belgian register of assets ("vermogensregister") and the possible violation of privacy in that regard.

On 19 September 2021, the Belgian Data Protection Authority published the Code of Conduct of 28 January 2021of the National Chamber of Notaries. This Code specifies certain modalities regarding the application of the GDPR for notaries.

Data protection in the pandemic

The Belgian Data Protection Authority has issued guidance and a FAQ page regarding all privacy and data protection related questions (see: https://www.gegevensbeschermingsautoriteit.be/burger/thema-s/covid-19).

The Belgian Regions have concluded several Collaboration agreements in this regard (e.g. on the vaccination strategy on the Belgian Covid Safe Ticket), on which the Belgian Data Protection Authority provided its comments (see: https://www.gegevensbeschermingsautoriteit.be/adviezen-rond-covid-19).

Public policy, public security and national security

In January 2021, the Belgian Constitutional Court issued a ruling in the context of the use of digital fingerprints on the electronic identity card (which were added in 2018, despite the negative opinion of the Data Protection Authority). The case was brought by the League for Human Rights on the grounds, inter alia, that the digital fingerprint was not legal, not proportionate and not secure. However, the Constitutional Court ruled that the purpose, to combat identity fraud, reasonably justifies an interference with the right to respect for private life and the protection of personal data. The fact that no permanent central register of all fingerprints would be introduced and that adequate safeguards were provided, constituted important elements in the decision. For more information – see: https://www.const-court.be/public/n/2021/2021-002n.pdf.

In April 2021, the Belgian Constitutional Court annulled Belgium's data retention law, which provided for an obligation to retain telecom data. An annulment decision was brought to the Constitutional Court against the reformed data retention law of 29 May 2016, where after the Constitutional Court posed preliminary questions to the Court of Justice, the latter rendering its judgment on 6 October 2020. In its ruling of April 2021, the Constitutional Court followed the judgment of the CJEU. For more information – see: https://www.const-court.be/public/n/2021/2021-057n.pdf.

EU data protection law in a global context

The Belgian Council of State has recently rendered two judgments following the Schrems II judgment.

In the first judgment, the Council of State suspended the execution of an award decision ("gunningsbeslissing") in summary proceedings because of a violation of the GDPR. The Council ruled that the contracting authority already has to consider GDPR-compliance in the regularity examination of a tender and externalize the results of such examination in the award decision. If the contracting authority indicates that the compliance with the GDPR by the chosen tenderer (in this case Amazon Web Services (AWS) - a cloud provider) is a "concern", then the contracting authority had to examine whether the chosen tenderer can guarantee the level of protection of personal data required by Union law. For more information – see: http://www.raadvst-consetat.be/Arresten/250000/500/250599.pdf.

In the subsequent judgment between the same parties, the Council of State rejected the claim to suspend the execution of the award decision. One of the loosing candidates filed a new claim for suspension in summary proceedings because the chosen candidate uses AWS. The Council ruled that the mere use of AWS and the transfer of data to the United States is not in itself prohibited if sufficient additional measures have been taken to provide adequate safeguards for the protection of personal data in the context of the transfer, including encryption of the data before it is transferred to AWS. The Council indicates that in this case the file shows that the chosen candidate does provide a comprehensive set of safeguards that can ensure the protection of personal data. For more information – see: RvS 19 augustus 2021, nr. 251.378 (not yet published).

Furthermore, the EDPB has provided a positive opinion on the Code of Conduct for Cloud Service Providers of the Belgian Data Protection Authority. The application for this Code of Conduct was made by Scope Europe, who wished to be accredited as a monitoring body for the EU Cloud code of conduct.

For the opinion of the EDPB on the Belgian Code of Conduct - see https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf.

AI, Gatekeepers and Data Altruism: situating data protection amongst new regulatory initiatives

Within the framework of the EU SOLID initiative, the Flemish government (Digital Flanders) is currently looking into the possibility of setting up a Data utility company ("Datanutsbedrijf") to explore the possibilities of providing the services around the offer of the personal data vaults to organizations and governments outside Flanders.

In April 2021, there also has been legislative proposal amending the law of 11 April 1994 on public access to government information, in order to provide more transparency on the use of algorithms by the government. For more information – see: https://www.lachambre.be/FLWB/PDF/55/1904/55K1904001.pdf.

General update: Cyprus

Written by: Professor Stéphanie Laulhé Shaelou and Dr. Katerina Kalaitzaki

Any other relevant developments that you wish to highlight

Law 125(I)/2018 of 31 July 2018 is the national law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data in Cyprus. Since the adoption of the law no legal amendments have been made to alter its text. Law 44(I)/2019 implemented the Data Protection Law Enforcement Directive (LED) (EU) 2016/680 into national law and again no legal amendments took place since its adoption on 27 March 2019.

However, the Office of the Commissioner for Personal Data Protection has issued 2 opinions (since the submission of the national report in 2019) providing guidelines and/or clarifying parts of the law addressed to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies. The second of these two opinions concern the use of programmes/software used by Higher Education Institutions due to the measures adopted to prevent the spread of the Covid-19 pandemic. The opinions have been issued in accordance with Article 58(3)(b) of the GDPR which grants each supervisory authority the authorisation and advisory power to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.

The first opinion (16 January 2020) since the submission of the national report for Cyprus (Topic 2), concerned the implementation of Article 10 of the GDPR (Processing of personal data relating to criminal convictions and offences) (http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%95%CF%81%CE%BC%CE%B7%CE%BD%CE%B5%CE%AF%CE%B1%20%CF%84%CE%BF%CF%85%20%CE%AC%CF%81%CE%B8%CF%81%CE%BF%CF%85%2010%20%CF%84%CE%BF%CF%85%20%CE%93%CE%9A%CE%A0%CE%94.pdf?openelement). In particular the opinion clarifies that "official authority" within the meaning of Article 10 GDPR is not clearly defined in the Regulation yet according to the text of the Article, in order for an organisation to be considered an "official authority", it must (a) have the power to exercise substantive control and (b) the exercise of control must be formal, ie it derives from national law. In Cyprus, the official Authority is the Police, which also keeps a complete criminal record, ie the Archive of Previous Convicts. In Cyprus, adequate guarantees

for the rights and freedoms of data subjects are ensured by Articles 9 and 10 (1) of the Police Law. Article 9 provides that the Record of Previous Sentences is kept for the purpose of issuing certificates criminal record or presentation of convictions before a competent court, in the context of criminal procedure, or fulfilment of the Republic's obligations arising from the European acquis, international convention or law in force in the Republic. Article 10 (1) provides that a criminal record shall be issued only to the applicant or to a person duly authorized by him. Under these provisions, where a public authority or a private body relies on any of the conditions of Article 6 (1) of the GDPR for the processing of data relating to criminal convictions and offenses or related security measures, such data may be collected by pursuant to Article 10 (1) of the Police Law, ie by issuing a criminal record to the applicant or to a person duly authorized by him.

The second opinion (21 August 2020) concerned the surveillance of distance / online examinations from higher education institutions addressing the concerns raised by students and organised representative groups on the use of programmes/software which examinees have to install on their computer (http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/CBD480CDE52BEF21C225820A004BBEB3/$file/%CE%93%CE%BD%CF%8E%CE%BC%CE%B7%201-2020%20-%20%CE%95%CF%80%CE%B9%CF%84%CE%AE%CF%81%CE%B7%CF%83%CE%B7%20%CF%84%CF%89%CE%BD%20%CE%B5%CE%BE%20%CE%B1%CF%80%CE%BF%CF%83%CF%84%CE%AC%CF%83%CE%B5%CF%89%CF%82%20%CE%B5%CE%BE%CE%B5%CF%84%CE%AC%CF%83%CE%B5%CF%89%CE%BD.pdf?openelement). Higher education institutions, in the context of conducting distance examinations via the internet, should act as follows:

1) To assess the necessity of using a surveillance program and adopt the use of such a program, after first studying the various alternatives. Depending on the institution, the course and the skills to be evaluated, alternatives may be applied such as:

- oral examination or homework assignment or examination with open books,

- enabling physical examinations to take place (e.g., for institutions with a small number of students),

- Separation of the examinees into smaller groups and use of more rooms or conducting the examinations in larger rooms

- Separation of the examinees into groups that will come to the examination on different days meaning that the examination essay will be different but of the same degree of difficulty

2) Refrain from implementing measures as a result of a decision taken solely on the basis of automated processing. In case the supervision program provides any indication, whether there is a possibility that the examinee has copied, the decision will be made by the teacher.

3) Apply the principle of data minimization throughout the process. For this purpose, they should disable the unnecessary functions of the program, so that the minimum is used for the satisfactory level of validity of the examinations and the data collected and processed in each type of processing to be achievement of the intended purpose. For this purpose:

a) there is no biometric identification of the examinees.

b) the examinees are asked to show on the camera the student identity card (where they exist), instead of the political identity card. In addition, depending on the institution / course and the skills to be evaluated, except in exceptional cases with special justification, the eye movements of the examinees are not controlled.

4) To fully inform the examinees about the processing of their data in accordance with Article 13 of the GDPR. The information should include the purposes of the processing, the legal basis of the processing, the recipients or categories of recipients, any transmission of the data to third countries, the retention period of the data and information on their rights. It is good practice for institutions to meet with student organizations and / or answer questions / concerns / concerns of examinees and consider possible solutions to alleviate their concerns before using such a surveillance program.

5) Ensure that the data collected are not used for any purpose other than to ensure the validity of the examinations.

6) Take appropriate technical and organizational measures for data protection, in accordance with Articles 5 (1) (f) and 32 of the GDPR, in order to ensure an appropriate level of security against risks, including, inter alia, the possibility of ensuring the confidentiality, integrity, availability and reliability of data.

7) Ensure that access to data is restricted to authorized persons only and that data flow is restricted to strictly restricted copies or registration points.

8) To pseudonymize personal data, where possible in each processing operation, so that the data can no longer be attributed to a specific data subject, without the use of additional information, provided that such additional information is kept separate and subject to technical and organizational measures to ensure that they cannot be attributed to an identified or identifiable natural person

9) To ensure that the personal data collected are kept only for the period necessary to achieve the purpose and in any case not more than 6 months from the date of the examination.

10) Select an appropriate surveillance program provider to provide adequate assurances for the implementation of appropriate technical and organizational measures, so that the processing meets the requirements of this Regulation and ensures the protection of the data subject's rights in accordance with Article 28 of the GDPR. To select the right provider, institutions should carefully study the provider's privacy policy and consider how they comply with the provisions of the Regulation, especially in the case of providers based in third countries.

11) In cases where the provider of the surveillance program is based in third countries and / or the data is stored on servers in a third country or in the cloud, take care to select the appropriate legal basis of Chapter V of the Regulation for the transmission of data to third parties Countries. The most appropriate legal basis is the use of standard data protection clauses issued by the Commission.

On 16 July 2020, the Court of Justice of the European Union (ECJ) issued a judgment abolishing the Privacy Shield, which made it possible for personal data to be transmitted to the United States. At the same time, he considered that the Standard Contractual Clauses remain in force, but with strict conditions. An organization that uses or intends to use them should review the monitoring status of the country and if a sufficient level of protection is not provided, it should not allow or suspend which transmission. Also, where necessary, it should take additional protection measures. Further guidance on this will be provided.

12) Carry out an impact assessment in accordance with Rule 35 of the Rules of Procedure to assess the risks and identify mitigation measures risks, taking into account all of the above issues.

No substantial impediments have been identified in the enforcement of the GDPR in Cyprus and or other barriers to its effective application nationally.

General update: Czech Republic

Written by: Vojtěch Bartoš

The Impediments to the enforcement of GDPR

- Lack of financial and personal resources on the side of the NSA

- Insufficient expertise of the NSA in ICT

- Systematic refusal of the NSA to shape the regulatory environment with ex-ante means (e.g. by issuing industry specific recommendations or guidelines)

- NSA not publishing its decisions in a comprehensive and systematic manner

- Grossly ineffective sanction policy of the NSA (not using its competences e.g. to impose temporary or definitive limitation/ban on processing or to issue substantive fines)

Data protection in the pandemic

The NSA issued between March 2020 and September 2021 several statements, recommendations and opinions with regard to processing of personal data in the context of the COVID-19 pandemic. The main focus of the statements was processing of personal data within the framework of the state-run "smart quarantine" and contact tracing, employees' health data in connection with compulsory COVID-19 testing, vaccination and other similar measures, covid passports/vaccination passports and other issues. The NSA also reported on some of these issues in other EU and non-EU states. In general, the role of the NSA during the pandemic was relatively active which helped to certain extent to data controllers (namely employers) to navigate through the maze of covid-19-related regulations and data protection rules. On the other hand, the NSA did not address in any way whatsoever the extensive and recuring ransomware attacks on some Czech hospitals during early 2020 although these attacks might have been some of the most notable data breaches in the Czech Republic since the GDPR came into effect.

The Ministry of Health issued since March 2020 several administrative measures of temporary nature which allowed/mandated processing of personal data namely for the purposes of contact tracing and "smart quarantine", compulsory testing of employees and other persons (students, clients and visitors of social care facilities, etc.). Almost no permanent legislative changes were made in order to provide for more specific legal bases of such processing, additional specifications of such processing activities or additional safeguards for the data subjects. Once these administrative measures are repealed most of these processing activities (namely processing of employees' health data) should be ceased. However, in the meantime many controllers stared assuming that further processing of such data (e.g. personal data related to covid-19 testing of employees) can be based on their legitimate interest. As a result, it can be observed in practice that covid-19-related health data are becoming "less private" and both public and private interests on their processing start prevailing. In that regard it can be seen as certain erosion of privacy.

General update: Greece

Written by: Virgina Tzortzi

The Impediments to the enforcement of GDPR

In terms of the provisions of Law 4624/2019 and their compatibility with the GDPR, Opinion 1/2020 of the HDPA identified several issues that render the national legislation problematic. For example, the legislator has adopted a distinction between the entities of the public and the private sector, a distinction that can lead to confusion of the notions of "data controller" and "data processor". Several national provisions, such as article 5 and 22, constitute a mere repetition of the Regulation's relevant provisions, contrary to the GDPR, while the second paragraph of article 22 provides for cases under which the processing of sensitive data is allowed, without such derogations being allowed by the GDPR. Another example of exceptions introduced by the national law contrary to the GDPR, is that of article 28 para. 2 of Law 4626/2019, which pertains to the processing of personal data for demographic, scientific and artistic purposes. The HDPA found the exceptions introduced under said article to be so broad that the core of the right to data protection being undermined.

Additionally, in July 2021 the HDPA issued its Annual Activity Report, in which it is identified that the process of adapting to the new framework set by the GDPR is still ongoing, and the information systems used by the Authority to deal with complaints and requests are under the process of being upgraded and extended. The lack of adequate personnel is mentioned as the most pressing challenge faced by the HDPA in carrying out its mission, and the Member State's obligation set forth in article 52 (4) GDPR to ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board, is not abided by.

Beyond NSAs: the role of other actors in developing data protection

Apart from the HDPA and other administrative authorities such as ADAE and EETT that deal with data protection issues, one cannot overlook the role of national court in developing data protection. The judicial decisions interpreting and applying Law 4624/2019, through which the GDPR and Directive 2016/680 were implemented into the national legal order, are critical in clarifying the content of the applicable legislation.

Additionally, and given that according to Decision 1/2020 of the HDPA, the documents and materials of a case pending before a national court do not constitute personal data subject to the supervision by the HDPA, the role of prosecutorial and judicial authorities in safeguarding data protection in the process of prevention, investigation, detection or prosecution of criminal offences is pivotal.

Data protection in the pandemic

Since the beginning of the pandemic, the Hellenic Data Protection Authority (has issued several guidelines pertaining to the processing of personal data in the process of managing the COVID-19 pandemic (Decision 5/2020 and Guidelines 1/2020) and to the adoption of data security measures in the context of teleworking (Guidelines 2/2020 and 1/2021).

Guidelines 1/2020 clarify the legal basis for the processing of personal data in the context of dealing with the pandemic and underline that the right to data protection is not absolute, but can be weighed against other rights, such as health and human life. The guidelines determine which data can be characterized as "health data" falling under the scope of article 9 GDPR and the conditions for their processing, while the also underline the need for anonymisation of the data that is published for statistical and demographic reasons.

Additionally, the gradual lifting of quarantine measures and the reopening of certain activities has been made conditional upon the vaccination of the public and businesses, such as restaurants or theaters,

are requested to verify whether their customers have been vaccinated, by requesting a vaccination certificate. The legislation that provided for the creation of a mobile application, used for the verification of the EU Digital COVID Certificates or vaccination certificates, was examined by the HDPA with regards to its compatibility with data protection rules. The HDPA issued Opinion 2/2021 identifying several issues of the proposed legislation relating to the lack of an impact assessment, the role of the Ministry of Health and the General Secretariat for Civil Protection as data controllers and the lack of clarity on the sanctions that will be imposed in cases of data breaches that occur in the use of the application. Interestingly enough, the relevant legislation was adopted by the Greek Parliament, without awaiting the delivery of the HDPA's opinion.

The guidelines for the application of data protection rules on teleworking were recently complemented by Guidelines 1/2021 . The HDPA underlines the obligation of the employer, as the data controller, to inform the employee on the benefits and downsides of teleworking and ensure that the processing of personal data takes place in accordance with the principles of article 5 GDPR. The HDPA also takes into account the disadvantageous position of the employees in the private sector and clarifies that the methods used by the employer for the organization of the work carried out from home should not lead to inequalities, discrimination or the adoption of automated decisions contrary to article 22 GDPR.

Technical and organizational measures should be put in place to ensure that the exercise of data subjects' rights is not hindered by teleworking, and any delays in their satisfaction are dully justified by the controller.

Additionally, the HDPA clarifies that the employer may use IT systems to verify whether the employees actually provide their services within the working hours, however the constant and generalized collection of personal data, e.g. through the compulsory activation of the computer's camera, the sharing of the employee's screen or the monitoring of keyboard/mouse movements, cannot be justified in accordance with the principle of proportionality.

General update: Italy

Written by: Francesco Rossi Dal Pozzo

Beyond NSAs: the role of other actors in developing data protection

On 26 May 2021, the Garante per la protezione dei dati personali (Italian Data Protection Authority) and the Garante nazionale dei diritti delle persone privati della libertà personale (Italian Guarantor for the Rights of Persons Detained or Deprived of Liberty) adopted a memorandum of understanding on the protection of persons deprived of their liberty. The two Authorities will cooperate to protect the dignity and rights of detainees and other persons under forms of restriction of freedom, such as migrants held in Centers for Return (Centri per i rimpatri) and guests in Residences for the Execution of Security Measures (Residenze per l'esecuzione delle misure di sicurezza). The two Authorities will be able to activate joint inspections and investigations on cases of mutual interest, initiate fact-finding investigations, exchange information on possible violations of relevance to the other Authority and support joint training projects to share experiences and improve specific skills in the field.

The Italian Data Protection Authority has also collaborated with the Italian Medicines Agency (AIFA) in the drafting of the Communication of 12 March 2020 on the management of clinical trials in Italy under Covid-19 emergency, to ensure an adequate level of protection of personal data in the context of the remote management of the monitoring phase of clinical trials of drugs.

Data protection in the pandemic

In the context of the Covid-19 pandemic, the Italian Data Protection Authority has adopted several measures aimed at achieving a fair balance between public health and the protection of personal data. These measures include: Measure authorizing the processing of personal data carried out through the Covid-19 Alert System - Immuni App (1 June 2020); Measure of 17 December 2020, concerning the "TuPassi", a system to book services or schedule appointments with public and private entities); Injunction order against Azienda Ospedaliera Regionale (Regional hospital) "San Carlo" of Potenza (27 January 2021); Injunction order against Azienda USL (local health authority) of Romagna (27 January 2021); Measure of 25 February 2021, regarding the activities and methods of processing personal data of politicians who have requested allowances allocated in reaction to Covid-19; Measure authorizing the processing of personal data carried out through the Covid 19- App Immuni Alert System following the update of the impact assessment carried out by the Ministry of Health on which the Authority had expressed its opinion in a measure of 1 June 2020 (25 February 2021); Order of injunction against the Municipality of Palermo (15 April 2021); Warning measure regarding the processing carried out in relation to the green certification for Covid-19 provided for by legislative decree 22 April 2021, no. 52 (23 April 2021); Injunction order against Synlab Med srl concerning the communication to mistaken recipient of Covid-19 test reports (13 May 2021); Measure warning the Campania region regarding the use of green certifications for Covid-19 (25 May 2021); Measure of 3 June 2021 regarding Mitiga app; Corrective measure against PagoPA regarding the functioning of the IO app (9 June 2021); Measure providing guarantees for the use of the IO App to access Covid-19 green certifications (17 June 2021); Measure of definitive limitation regarding the processing of green certifications for Covid 19 provided by the Autonomous Province of Bolzano (18 June 2021); Measure warning the Region of Sicily with regard to the processing of personal data resulting from additional measures for the epidemiological emergency from Covid-19 (22 July 2021).

The shift of a large part of daily activities online, induced or accelerated by the pandemic, has also represented the target of significant consultative and guidance activities of the Authority, aimed at ensuring the necessary guarantees. These include: Opinion on the draft ordinance containing urgent civil protection provisions in relation to the emergency on the national territory concerning the health risk connected to the onset of pathologies deriving from transmissible viral agents (2 February 2020); Opinion on the modalities of delivery of the electronic medical prescription (19 March 2020); Distance teaching: first indications (26 March 2020); Opinion to the Ministry of Economy and Finance on a draft decree, to be adopted in agreement with the Ministry of Health, on the dematerialization of the prescription for pharmaceutical services not charged to the National Health Service and on the modalities of consultation by the patient of the dematerialized memo of the electronic prescription (2 April 2020); Opinion on the outline of the provision of the Director of the Italian Revenue Agency (Agenzia delle Entrate) concerning the access to the pre-compiled declaration by taxpayers and other authorized parties, starting from the fiscal year 2019 (23 April 2020); Personal data flows between INPS (National Institute for Social Security) and the Campania Region in the context of the provision of economic support measures (28 April 2020); Opinion on proposed legislation to provide for an application to track COVID-19 infections (29 April 2020); Opinion on an outline of a regulatory provision to allow seroprevalence surveys on SARS-COV-2 to be conducted by the Ministry of Health and ISTAT (Italian National Institute of Statistics) for epidemiological and statistical purposes (4 May 2020); Opinion to the Autonomous Province of Trento on the draft provincial law concerning further support measures for families, workers and economic sectors related to the epidemiological emergency from COVID-19 and consequent variation to the budget of the Autonomous Province of Trento for the financial years 2020-2022 (8 May 2020); Measure on INPS data breach: Communication to affected stakeholders (14 May 2020); Opinion on a draft decree regarding the processing of personal data carried out through the

Sistema Tessera Sanitaria (Italian Health Insurance Card) as part of the Covid-19 alert system (1 June 2020); Personal data protection impact assessment submitted by the Ministry of Health regarding the processing carried out as part of the Covid-19 alert system called 'Immuni' - Note on technological aspects (3 June 2020); Processing of personal data as part of the Covid-19 emergency by Offices of notifications, Executions and Protests (Ufficio Notifiche Esecuzioni e Protesti) of national courts (9 June 2020); Opinion on the request for civic access - data concerning the distribution of cases of Covid-19 registered in the region of Valle d'Aosta (3 September 2020); Opinion to the Autonomous Province of Trento on an outline of regulation concerning reactive medicine (medicina di iniziativa) in the provincial health service (1 October 2020); Opinion on the draft decree of the Ministry of Economy and Finance and the Ministry of Health on the implementation modalities of the reporting system of rapid antigenic swabs by family doctors and pediatricians and on the provision of these electronic reports to the subjects referred to in art. 19 of law decree no. 137/2020, through the Health Insurance Card System (3 November 2020); Opinion on an outline of the order of the Extraordinary Commissioner for the implementation and coordination of the measures necessary for the containment and contrast of the epidemiological emergency COVID-19 (17 December 2020); Opinion on an outline of a provision that aims to regulate the information systems functional to the implementation of the strategic plan of vaccines for the prevention of SARS-CoV-2 infections (13 January 2021); Opinion on a draft decree of the Ministry of Economy and Finance and of the Ministry of Health, amending the decree of 3 June 2020, concerning the technical modalities for the involvement of the Health Insurance Card System for the purposes of implementing prevention measures in the context of public health interventions related to the Covid-19 emergency (25 February 2021); Opinion on a request for civic access (FOI, 23 April 2021); Guidance document on the designation, position and duties of the Data Protection Officer (DPO) in the public sector (19 April 2021); Opinion on the prime ministerial decree for the implementation of the digital Covid certificate national platform for the issuance and verification of Green Pass (9 June 2021); Opinion on the draft Directive of the President of ISTAT on Identification of the processing of personal data referred to in Articles 9 and 10 of Regulation (EU) 2016/679 in the context of alert-cov statistical work (24 June 2021); Opinion on the draft decree on Measures setting out amendments and additions to the implementing provisions of Article 9, paragraph 10, of Decree-Law 22 April 2021, no. 52 on Urgent measures for the gradual recovery of economic and social activities in compliance with the need to contain the spread of the COVID-19 pandemic (31 August 2021).

Public policy, public security and national security

It is worth noting the entry into force of Law 4 August 2021 no. 109, "Conversion into law, with amendments, of Law Decree 14 June 2021 no. 82, containing urgent provisions on cybersecurity, definition of the national cybersecurity architecture and establishment of the Agency for national cybersecurity" (Official Journal of the Italian Republic, General Series no. 185 of 4 August 2021). The new legislation, effective as of 5 August 2021, defines the national cybersecurity architecture and establishes the National Cybersecurity Agency. Specifically, the law consists of nineteen articles.

Articles 1 to 4 define the national cybersecurity system, which is headed by the President of the Council of Ministers, who is given the overall direction and responsibility for cybersecurity policies, as well as the adoption of the relevant national strategy and - subject to deliberation by the Council of Ministers - the appointment and revocation of the Director General and Deputy Director General of the new 'Agency for National Cybersecurity' (established by Article 5). The Parliamentary Committee for the Security of the Republic (COPASIR) and the competent parliamentary commissions are informed in advance of these appointments (article 2). The President of the Council of Ministers may empower the Delegated Authority for the Information System for the Security of the Republic, where established, to perform those functions that are not exclusively attributed to him (article 3).

The "Inter-ministerial Committee for cybersecurity" (CIC) is established at the Presidency of the Council of Ministers. This body has the function of consulting, proposing and supervising cybersecurity policies (article 4).

Article 5 provides for the establishment of the National Cybersecurity Agency; article 6 regulates its organization; article 11 deals with its financial resources and accounting autonomy; article 12 concerns its personnel. Article 14, which deals with the annual reports that the President of the Council of Ministers is required to send (to Parliament and COPASIR) on the activities of National Cybersecurity Agency. Within the latter, the constitution of a "Nucleus for cybersecurity" is envisaged to deal with possible crisis situations (Articles 8 and 9). Article 10 addresses the management of crises involving aspects of cybersecurity.

Article 13 concerns the processing of personal data for national cyber security purposes. Article 15 dictates a series of novelties to Legislative Decree no. 65 of 2018 (implementing Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union) in order to harmonize it with the regulatory framework inherent in Law Decree 14 June 2021 no. 82. Article 16 amends other legal provisions for the same purpose.

EU data protection law in a global context

The Italian Data Protection Authorities has also addressed the area of personal data transfers to third countries. It mainly focused on the innovations introduced following the adoption by the CJEU of the so-called 'Schrems II' ruling (see Case C-311/18) and the documents of the European Data Protection Board with recommendations on measures to ensure compliance with the GDPR in the context of cross-border data transfers. These Italian Data Protection activities include:

1) Collaboration between the Italian Data Protection Authority and other European supervisory authorities as part of a task force in charge of coordinating the examination of 101 complaints lodged against various data controllers established in the EEA member states regarding the use, via their websites, of services provided by Google and Facebook that involve the transfer of users' personal data to the United States. In this context, and with specific reference to the complaints received by the Italian Data Protection Authority, a preliminary investigative activity was launched to acquire more elements regarding the guarantees adopted by the data controllers and managers involved after the declaration of the CJEU regarding the invalidity of Commission Decision No. (EU) 2016/1250 (so-called EU-US - Privacy Shield) for the purposes of transferring data subjects' data overseas.

2) The activity of evaluating the requests received regarding the approval of Binding Corporate Rules (BCR) pursuant to art. 47 of the GDPR, aimed at requesting the involvement of the Italian Data Protection Authority as leader in the evaluation of the BCR. In particular, the role of the Italian Data Protection Authority as leader in the European cooperation procedure was formalized in relation to a proceeding concerning a multinational group of companies in the digital infrastructure sector, after verification of the existence of the requirements set out in WP 263 (Working Document of Article 29 Working Party of 11 April 2018). In this capacity, an initial articulated analysis of the documents received was carried out, also through frequent interlocutions with the group aimed at making the necessary changes to the text of the proposed BCR to include all the elements indicated by WP 256 (Working Document of Article 29 Working Party of 6 February 2018) and, more generally, to conform the same to the GDPR; also for the purpose of their subsequent transmission (pursuant to art. 57, par. 1, letter g of the GDPR), to the supervisory authorities identified as co-reviewers within the relative European cooperation procedure.

3) Advisory activity on various queries received with regard to the provisions of Chapter V of the GDPR concerning, among other things, the use of exemptions in specific situations (see Art. 49 of the GDPR), the application of the standard data protection clauses pursuant to Art. 46, paragraph 1, letter c), of the GDPR, binding corporate rules and their approval pursuant to Art. 47 of the GDPR.

AI, Gatekeepers and Data Altruism: situating data protection amongst new regulatory initiatives

In the field of Artificial Intelligence, it is worth noting the fact-finding survey on Artificial Intelligence launched, on 13 May 2020, by the Joint Committees VIII and X of the Senate, pursuant to article 48 of the Rules of Procedure.

At the same time (2 June 2020), the Ministry of Economic Development launched the Italian Strategy for Artificial Intelligence. The Strategy is structured in three parts: the first is dedicated to the analysis of the global, European and national markets for Artificial Intelligence. The second part describes the fundamental elements of the strategy, while the third one deepens the proposed governance of Italian AI and makes some recommendations for the implementation, monitoring and communication of the national strategy on artificial intelligence, which is clearly anthropocentric and oriented towards sustainable development.

Last, as confirmation of the role played in this context by the Italian Data Protection Authority, it is worth noting that on 23 June 2021, the President of the Authority for the protection of personal data, Prof. Pasquale Stanzione, intervened in a hearing at the IX Commission of the Chamber of Deputies (Transport, Post, Telecommunications) on the subject of the complex relationship between users/consumers and profiling techniques with AI technology adopted by the Gatekeepers (see Tecnica, protezione dei dati e nuove vulnerabilità relazione del Presidente Pasquale Stanzione, Rome, 2 July 2021).

Any other relevant developments that you wish to highlight

The Data Protection Authority's track record of GDPR enforcement, from 25 May 2018 to 30 June 2021, includes:

- DPO contact information disclosures: 60,864.

- Complaints and reports: 30,262.

- Data breach notifications: 4,465.

The Data Protection Authority imposed the following corrective measures and sanctions (art. 58(2) GDPR) in 2020:

- Warnings to controller/processor (art. 58(2)(a) GDPR): 6.

- Warnings to controller/processor (Art. 58(2)(b) GDPR): 45.

- Injunctions to data controller/processor to comply with requests made by data subjects concerning the exercise of rights granted by the GDPR (Art. 58(2)(c) GDPR): 23.

- Injunctions to the controller to comply with the provisions of the GDPR (art. 58(2)(d) GDPR): 16.

- Injunctions to data controller to notify the data subject of a personal data breach (Art. 58(2)(e) GDPR): 2.

General update: The Netherlands

Written by: Dominique Hagenauw

The Impediments to the enforcement of GDPR

In 2020, the AP imposed 7 administrative fines pursuant to Article 83 GDPR, 2 administrative enforcement orders under periodic penalty payment and issued 4 reprimands against private companies, public authorities and other organisations.

Since the publication of the FIDE Congress Volume, the details of the following administrative fines have been published:

· TikTok fined for violating children's privacy (€ 750,000).

· Employee Insurance Agency fined for not properly securing the sending of group messages (€450.000).

· Orthodontic practice fined for unsecured patient website (€12,000).

· Maintenance company CP&A fined for violating privacy of sick employees (€15,000).

· Locatefamily.com fined for not having a representative in the EU (€525,000).

· Overijssel chapter of the Freedom Party (PVV) fined for failing to report data breach (€7,500)

· Municipality of Enschede fined for using Wi-Fi tracking (€600,000)

· Booking.com fined for delay in reporting data breach (€475,000)

· Hospital fined for inadequate protection of medical records (€440,000)

· National Credit Register (BKR) fined for personal data access charges (€830,000).

· Company fined for processing employees' fingerprint data (€725,000).

· Tennis association KNLTB fined for selling the personal data of its members (€525,000).

Regarding the AP itself, the AP has repeatedly called for more budget and capacity to be able to step up their enforcement. After the general elections in March 2021 and following two motions adopted by Parliament calling for an increase of the AP's budget, the AP sent a position paper to the informateur (a mediator who explores which parties could form a new government) in which the AP requests a fourfold increase of its budget to 100 million euros per year to be able to perform its work properly.

Beyond NSAs: the role of other actors in developing data protection

GDPR administrative case law is growing. There have been two court decisions in proceedings on the merits regarding an administrative fine imposed by the AP:

• In November 2020, the Middle Netherlands District Court annulled the fine of €575,000 imposed on the football streaming service provider VoetbalTV for not being able to rely on a legitimate interest when processing personal data for purely commercial interests and profit maximisation. According to the court, the journalistic exception does not apply in view of the fact that the broadcast contains too little news value. However, the court does find that the fact that the claimant has a commercial interest does not automatically mean that they cannot have a legitimate interest. Excluding a particular interest as a legitimate interest in advance is contrary to European case law. The court ruled, inter alia, that this interpretation of legitimate interest by the AP was too strict. An appeal is pending before the Administrative Jurisdiction Division of the Council of State.

• In March 2021, the Hague District Court upheld the enforcement decision against a hospital in The Hague for insufficient internal security of patient records, but reduced the fine to €350.000. The AP had issued the fine on a hospital for failing to adequately protect patients' personal data. They had established that the hospital lacked two-factor authentication and that the logging of access to patient files was not controlled on a regular basis. As reasons for lowering the fine, the court referred to the fact that the hospital did have measures in place to prevent unauthorized employees having access to patient files, and that the hospital did introduce two-factor authentication and proper logging after receiving the fine, showing a willingness to address the problem.

The GDPR has also been invoked, for the first time, in a civil law dispute among two businesses competing on the same market (GPS-watches for elderly and dependant people). In February 2021, a Dutch civil law court ruled that a distributor of GPS-watches could not invoke the protection offered by the GDPR against a competitor on the same market. The court held that, in spite of the fact that competitors relying on the GDPR to protect their interests would contribute to the enforcement of the GDPR, in the circumstances of the case the interests of the complainant were not protected by the GDPR and could therefore not be invoked against its competitor. Before initiating judicial proceedings, the claimant had made a complaint with the AP concerning the same matter. The AP informed that they will not process the complaint, because these parties do not have the right to complain.

Data protection in the pandemic

The battle against the pandemic has raised a lot of new issues relating to human rights including privacy. Often a balancing of colliding rights was necessary. In the Netherlands, measures battling covid having an effect on privacy have been the release of the apps 'CoronaMelder' and 'CoronaCheck'. Both have been regulated by new legislation approved by the Dutch Parliament:
• The CoronaMelder app is designed to alert the user when they have been in the proximity of someone (who remains unknown to the user) who has reported themselves as covid positive. This allows the users to take precautionary measures even if they have not yet shown symptoms. The app does not track someone's location or identity and the use is entirely voluntary. The AP in its advice found that the government should enter into an agreement with Google and Apple regarding the software they deliver to use the app, that there should be a law to regulate the use of the app and that it should be clear that the servers used by the app are secure.
• The CoronaCheck app is not linked to the CoronaMelder app, as this app does use personal data to show that the user has either been vaccinated, negatively tested or recovered from covid. The app does not reveal which of these is applicable but only shows a generic QRcode. The code is temporary and the person checking this code cannot download it. Only the personal data necessary to check the person's identity is shown. The AP has also published its advice on this app, relating to consent that needs to be freely given (where this is the legal ground), possible voluntary access policies, identifying data, etc.

Furthermore, owners of cafes and restaurants had to compulsory offer visitors to register their information in order to contact them in case another visitor would be diagnosed with covid after his or her visit. For visitors, the law however stipulated that registering was voluntarily and refusal without consequences.

Also, the use of Telecommunication data (location data) in the battle against covid was a topic of discussion in the Netherlands and a draft law was submitted to parliament, which has put it on hold pending the installation of a new government. In its advice, the AP has asked for strict limitations in this regard.

A new issue that has not been resolved yet is the call from employers to register their employee's covid

status. So far this is prohibited by law, but it's currently under debate whether or not this should be made legal, at least for specific groups like medical staff.

Public policy, public security and national security

The rulings of the CJEU of 6 October 2020, Privacy International (C 623/17, EU:C:2020:790), and in Joined Cases La Quadrature du Net and Others (C 511/18, C 512/18 and C 520/18) had effect on the Intelligence and Security Services Act 2017 (Wiv). As a result of these rulings, it can be concluded that the Wiv does not completely fall outside of the scope of application of EU data protection law, at least as far as it concerns the analysis of bulk data, in case of data retention by private parties. However, although the ramifications of the abovementioned CJEU cases need more clarification in the future, according to experts, the Wiv probably does not need to be amended on this point.

The Wiv provides safeguards related to automated analysis of bulk data. It is considered to be a 'special power'. Special powers may only be applied for the performance of a narrower set of tasks, such as defending a continuing democratic legal order, protecting national security, investigating other countries and their militaries, maintaining international legal order, or specific military activities. The application of the special power at hand not only needs prior consent of the minister, but also requires an additional prior consent from an independent and specialized judicial commission, the Review Board for the Use of Powers (TIB). The Review Committee for the Intelligence and Security Services (CTIVD) performs an ex post control.

AI, Gatekeepers and Data Altruism: situating data protection amongst new regulatory initiatives

A proposal of the European Commission for a Data Governance Act (DGA) would provide the possibility to individuals or companies to give consent for so-called "data altruism", in order to share the data they generate for the common good, voluntarily and free of charge (e.g. for scientific research, Healthcare etc). Various questions have been raised with respect to data altruism. For example, the EDPB and the EDPS recommend that the DGA should better define the purposes of general interest of such "data altruism". Data altruism should be organised in such a way that it allows individuals to easily give, but also, withdraw their consent.

The proposal is also discussed in the Netherlands and questions have been raised in the Dutch Parliament concerning the conditions that apply to guarantee the quality and reliability of organisations that focus on data altruism. The government furthermore feels that in relation to the proposed European label for data altruism organisations, attention should be paid to the risk of improper use of donated data or uninformed donations of data. A code of conduct is suggested to help in mapping the interests of those involved and translate these into concrete conditions, which data altruism organisations must then commit to in order to obtain the label.

Any other relevant developments that you wish to highlight

In 2021, the AP warned that it was seeing an explosive increase in the number of hacks aimed at stealing personal data. The number of reports in 2020 was 30% higher than in the previous year.

General update: Switzerland

Written by: Jacques Beglinger

The Impediments to the enforcement of GDPR

1.1. Only partial applicability of the GDPR for Switzerland

Switzerland is not a member of the European Economic Area (EEA), but is linked to it and the European Union through a network of bilateral or sectoral agreements. This means that European secondary law, and thus e.g. the GDPR, is only applicable to Switzerland where this results from a contractual obligation. For example, where Switzerland is covered by the Schengen and Dublin agreements, see printed Swiss Country Report, p. 599 et seq. There, Switzerland has implemented the EU requirements with the Schengen Data Protection Act (SDSG). The SDSG entered into force on 1 March 2019.

1.2. Accession of Switzerland to the modernized Convention 108 of the Council of Europe

Switzerland's international understanding of data protection is traditionally based on the principles developed within the framework of the proceedings of the Council of Europe, as laid down in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), see [https://www.coe.int/en/web/data-protection/convention108-and-protocol].

As already explained in the printed Swiss Country Report (see p. 598), the Swiss Federal Council decided on 30 October 2019 to sign the "Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Council of Europe Convention 108+). This signature was deposited with the Council of Europe in Strasbourg on 21 November 2019.

The Swiss Federal Parliament gave the necessary approval to the signature on 19 June 2020 (see Parliamentary item of business 19.086 [https://www.parlament.ch/en/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20190068].

According to Art. 141(3) Swiss Federal Constitution, international treaties are subject to a referendum if they contain important legislative provisions or if their implementation requires the enactment of federal laws. Therefore, the parliamentary resolution [https://www.fedlex.admin.ch/eli/fga/2020/1311/fr] was subject to an optional referendum, which, however, was not requested within the deadline of 8 October 2020.

Following the parliamentary decision, the Swiss Federal Council is thus authorised to ratify the protocol for Switzerland. It is expected to do so simultaneously with the entry into force of the revFDPA (see below) in the second half of 2022.

1.3. Autonomous alignment of Swiss data protection legislation with the GDPR

Currently, the Federal Act on Data Protection of 19 June 1992 (henceforth "FADP" or, according to some translations, "FDPA") is still in force in Switzerland (with i.a. important revisions of 24 March 2006 and 19 March 2010), see [https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en]. This law is based on the principles of Convention 108 of the Council of Europe as not yet modernised.

Against the background of the modernisation of the Council of Europe Convention on Data Protection No. 108 and in view of the innovations in EU data protection law, however, Swiss data protection law has been undergoing a transformation. To this end, the Swiss Federal Council submitted a draft for a full revision of the Federal Act on Data Protection (henceforth "revFADP" or, according to some translations, "revFDPA") to the Swiss Federal Parliament on 15 September 2017, see [https://www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2017/2017-09-150.html].

At the time of the conclusion of the printed Swiss Country Report, the total revision of the FDPA was still in progress (see printed Swiss Country Report, p. 598). In the meantime, it has been completed with parliamentary adoption of 25 September 2020 (see Parliamentary item of business 17.059 [https://www.parlament.ch/en/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059]. The

possibility under Swiss constitutional law to demand a referendum on the new law was not used. The corresponding deadline expired on 14 January 2021. The total revision is thus legally concluded. The full text has so far been published in the official languages French, German and Italian [https://www.fedlex.admin.ch/eli/fga/2020/1998/fr]. An unofficial English translation by the federal authorities is currently not available; for a private unofficial English translation, please refer to [https://datenrecht.ch/ndsg-en].

The new law is not yet in force. The Federal Council determines the date of entry into force (Art. 74(2) revFDPA). According to the authorities, entry into force is expected in the second half of 2022 (see e.g. suggested by the Swiss FDPIC, The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contracts, 27 August 2021, sect. 1 [https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Paper%20SCC%20def.en%2024082021.pdf.download.pdf/Paper%20SCC%20def.en%2024082021.pdf].

The revFDPA will be accompanied by an Implementing Decision (rev Ordinance to the Federal Act on Data Protection, revDPO), a draft of which has been published for public consultation on 23 June 2021, see [https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-84103.html].

With the entry into force of the revFDPA, the SDSG (see above), which is currently already in force, will be fully integrated into the revFDPA in terms of its content and will therefore be formally repealed at that time (Art. 68 revDPA in conjunction with Annex 1(I)).

The update format used here does not lend itself to an in-depth presentation of the revision changes. For a compact overall view of the content of the future revFDPA, however, see the FDPIC report "The new FADP from the FDPIC's perspective" of 5 March 2021 [https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-2053438021].

1.4. Adequacy regime

Another reason for aligning Swiss data protection regulations with the principles of the GDPR was to maintain the Swiss Adequacy Decision adopted by the EU Commission back in the year 2000 regarding the then valid Directive 95/46/EC also under the GDPR regime (see printed Swiss Country Report, p. 600 et seq).

As Switzerland has fully completed the preparations for ratification of the Modernisation Protocol 223 to the Council of Europe Convention 108+ (see above), an important prerequisite for renewal of the Swiss Adequacy Decision has been met (see Recital 105 of the GDPR).

On maintaining preexisting adequacy decision under the GDPR, the EU Commission has so far - despite the time limit in Art. 97(1) and (2)(a) - only published a general report (COM(2020) 264 final, sec. 2) of 24 June 2020, which indicates: «[…] As part of the first evaluation of the GDPR, the Commission is also required to review the adequacy decisions that were adopted under the former rules. The Commission services have engaged in an intense dialogue with each of the 11 concerned third countries <one of which is Switzerland> and territories to assess how their data protection systems have evolved since the adoption of the adequacy decision and whether they meet the standard set by the GDPR. The need to ensure the continuity of such decisions, as a key tool for trade and international cooperation, is one of the factors that has prompted several of these countries and territories <so as Switzerland> to modernise and strengthen their privacy laws. Additional safeguards are being discussed with some of these countries and territories to address relevant differences in protection. However, given that the Court of Justice in a judgment to be delivered on 16 July may provide clarifications that could be relevant

for certain elements of the adequacy standard, the Commission will report separately on the evaluation of the existing adequacy decisions after the Court of Justice has handed down its judgment in that case. […]»

The announced separate report has currently not yet been produced by the EU Commission and therefore the extension decision regarding the adequacy of the Swiss data protection regulation remains pending at the time of writing this Update.

Data protection in the pandemic

Various aspects of data protection played an important role in handling the pandemic in Switzerland. The development and use of Covid apps as well as government and scientific access to health data in Switzerland (which has a markedly federal structure which entails a certain independence of the Cantons in data protection matters, too) took up a lot of space in the media and in the social discussion (see for the latter inter alia Swiss Internet Governance Forum 2021, Sess. 2 [https://igf.swiss/wp-content/uploads/2021/07/SwissIGF_Messages-from-Berne-2021_en.pdf]).

A good overview of the challenges to data protection in Switzerland in times of Covid can be found in the 28th Annual Report 2020/21 of the FDPIC, see [https://www.edoeb.admin.ch/edoeb/en/home/documentation/annual-reports/28--taetigkeitsbericht-2020-2021.html], which addresses namely:

- The FOPH's access to Swisscom mobility data;

- Data protection challenges of introducing facilita- tions for people who have been vaccinated;

- Implementation of a data protection-compliant COVID-19 certificate;

- The Swiss proximity tracing app (SwissCovid app);

- The legal framework for collecting contact details;

- Data protection aspects of working from home;

- Data protection requirements for early detection of coronavirus in the workplace;

- Legislative process for the transposition of the COVID-19 Loan Guarantees Ordinance into the Federal COVID-19 Loan Guarantees Act;

- The FDPIC's duties and resources in times of Covid.

Public policy, public security and national security

4.1. Public security and national security

While the FADP as well as the revFADP in principle oblige both, private and federal authorities, to observe data protection (Art. 2(1) revFADP), federal authorities - and thus also those entrusted with safeguarding national security - may process personal data to the extent that they are specifically authorised to do so by a law (Art. 34 revFADP).

In this respect, the Federal Act on the Intelligence Service (Intelligence Service Act, IntelSA, [https://www.fedlex.admin.ch/eli/cc/2017/494/en]) of 25 September 2015 concerning the activities of the Federal Intelligence Service (FIS) is of particular importance with regard to safeguarding national security. Under the IntelSA, the FIS is permitted, in deviation from the revFADP in certain specified situations, to gather information from sources that are publicly and non-publicly accessible, to gather personal data without this coming to the attention of the persons concerned and use information

gathering measures which do and do not require authorisation (Art. 5 IntelSA). It shall, however, choose the information gathering measure that causes the least interference with the fundamental rights of the persons concerned and it may not gather or process any information relating to political activities or the exercise of freedom of speech, assembly or association in Switzerland. Moreover, proportional duties to delete data recorded apply.

See also the comments on section 5.1 of this Update report «Effects of the Schrems II case law of the European Court of Justice on Swiss data protection law", below, as well as the Swiss FDPIC's "2nd CH-US Privacy Shield Report" of 9 March 2020, section 2 "Authorities' access to personal data for national security", [https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2020/PS%20Bericht%202019%20EN.pdf.download.pdf/PS%20Bericht%202019%20EN.pdf].

For the surveillance of telecommunications, see the Federal Act on the Surveillance of Post and Telecommunications (SPTA, https://www.fedlex.admin.ch/eli/cc/2018/31/en) of 18 March 2021. Under it, the Swiss Confederation shall operate a Service for the surveillance of post and telecommunications under Article 269 of the Swiss Criminal Procedure Code8 (CrimPC). The Service, the ordering authorities, the approving authorities and the providers of postal and telecommunications services may process the personal data, including sensitive personal data and personality profiles, that they need to order, approve and carry out surveillance (Art. 4 SPTA).

Information processing specific to general police tasks is regulated in Art. 14 Federal Act on Measures to Safeguard Internal Security (FAMSIS, [https://www.fedlex.admin.ch/eli/cc/1998/1546_1546_1546/fr]).

Furthermore, on 18 December 2020, the Federal Parliament adopted the Federal Act on Information Security (FAIS) [see https://www.parlament.ch/en/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170028] which addresses the handling of own data by federal authorities specifically and complements the other mentioned acts in various aspects. Since no referendum has been requested by 10 April 2021, the text is thus legally concluded. The date of entry into force has not yet been determined as the respective Implementing Decision must first be drafted. Concerning specifically the processing of personal data in the information security context, see there Section 5 (Arts. 45 et seq. FAIS).

4.2. Cybersecurity in particular

On 27 May 2021, the Swiss Federal Council enacted the Ordinance on Protection against Cyber Risks in the Federal Administration (Cyber Risks Ordinance, CyRV, [https://www.fedlex.admin.ch/eli/cc/2020/416/en], which regulates the organisation of the Federal Administration for its protection against cyber risks as well as the tasks and responsibilities of the various offices in the cyber security domain. It addresses inter alia all intelligence and military measures designed to protect critical systems, to defend against attacks in cyberspace, to ensure the operational readiness of the Armed Forces in all situations, and includes active measures to recognise threats, to identify aggressors and to disrupt and stop attacks (see Art. 6 CyRV).

Moreover, it is worth mentioning that the revFDPA (see above) not only imposes obligations to take appropriate technical and organisational measures regarding data security commensurate with the risk (Art. 8 revFDPA). Rather, their deliberate disregard by private individuals will now be subject to direct individual punishment (Art. 61(c) revFADP). This means stricter sanctions in this respect, not only in comparison to the Council of Europe Convention 108+ (Art. 10 of which generally requires only "appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this

Convention"), but also in comparison to the GDPR, which does not provide for individual sanctions. The data security obligations to be complied with will be defined by the Federal Council in an Implementing Decision, which is currently still at the draft stage (see Arts. 1 et seq. revDPO, []https://www.bj.admin.ch/dam/bj/fr/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vorentw.pdf]).

EU data protection law in a global context

5.1. Effects of the Schrems II case law of the European Court of Justice on Swiss data protection law

The ruling of 16 July 2020 by the CJEU in the case C-311/18 Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems (henceforth Schrems II ruling) declared the Adequacy Decision 2016/1250 by the EU Commission regarding US companies certified under the EU-US Privacy Shield regime invalid. Since Switzerland is not a member of the EU, this ruling is not binding for Switzerland. Switzerland, however, maintains a parallel CH-US Privacy Shield (see, [https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t000000079Gr]). Hence the need for clarification arose in Switzerland, too.

While the FDPIC does not have the competence to invalidate the Swiss-U.S. Privacy Shield Framework (and its position is subject to any rulings to the contrary by Swiss courts), as part of its annual review of the Swiss-U.S. Privacy Shield Framework, the FDPIC, it concluded on 8 September 2020 that the Swiss-U.S. Privacy Shield Framework does not provide an adequate level of protection for data transfer from Switzerland to the US pursuant to the FADP, see [https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-80318.html] and published a Policy paper, including practical advice for Swiss companies, on the same date, see [https://www.newsd.admin.ch/newsd/message/attachments/64261.pdf]. Conversely, the US Department of Commerce also issued a clarifying notice to inform about this development, see [https://www.privacyshield.gov/Program-Overview].

In view of the above, in practice, companies may no longer rely on the Privacy Shield framework as a valid data transfer mechanism.

In the same document of 8 September 2020, the FDPIC expanded on the CJEU ruling and took the view that the use of alternative data transfer mechanisms, such as Standard Contractual Clauses (“SCCs”) or Binding Corporate Rules, which are frequently used in Switzerland, requires companies to conduct an assessment and possibly implement additional safeguards (including technical measures that can effectively prevent authorities in the receiving country from accessing the transferred data, such as encryption) where the risk assessment indicates that personal data is not adequately protected.

5.2. Standard Contractual Clauses

Following the adoption of Implementing Decision (EU) 2021/914 of 4 June 2021, by which, regarding the effect of the EU GDPR, the previous set of standard contractual clauses of 2010 was repealed, the Swiss FDPIC followed suit.

Along a first Communication of 18 June 2021 (see [https://www.edoeb.admin.ch/edoeb/en/home/data-protection/handel-und-wirtschaft/transborder-data-flows.html]), the FDPIC issued a “Guide to checking the admissibility of direct or indirect data transfers <from Switzerland> to foreign countries (Art. 6 para. 2 letter a FADP)”, see [https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%Bcbermittlungen%20mit%20Auslandbezug%20EN.pdf.download.pdf]

In a further Communication of 27 August 2021, it stated: "[…] the <Swiss> FDPIC recognises the standard contractual clauses for the transfer of personal data to third countries in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (pursuant to Implementing Decision 2021/914/EU) as the basis for personal data transfers to a country without an adequate level of data protection, provided that the necessary adaptations and amendments are made for use under Swiss data protection law. […]", [https://www.edoeb.admin.ch/edoeb/en/home/latest-news/aktuell_news.html#-1259254222]

At the same occasion, the FDPIC published a Guidance document of the same date "The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contracts", see [https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Paper%20SCC%20def.en%2024082021.pdf.download.pdf/Paper%20SCC%20def.en%2024082021.pdf]. In this document he explains the adaptations that are necessary in order for the <EU> SCCs to comply with Swiss legislation and thus be suitable for ensuring an adequate level of protection for data transfers from Switzerland to a third country in accordance with Article 6(2)(a) FDPA (or with Art. 16(2)(d) revFDPA once in force, respectively).

The necessary amendments to the EU SCC concern in particular the designation of the competent supervisory authority in Annex I.C under Clause 13, the applicable law for contractual claims under Clause 17 and of the place of jurisdiction for actions between the parties pursuant to Clause 18 b as well as adjustments or additions concerning the place of jurisdiction for actions brought by data subjects and concerning references to the GDPR. Until the revFDPA enters into force in the second half of 2022, there also needs to be a transitional provision concerning the protection of legal persons that still exists today under the current FADP but will no longer exist thereafter.

5.3. Impact of the Brexit

With the departure of the United Kingdom from the EU on 31 December 2020, the applicability of the GDPR to the UK also ended, as did the mutual facilitations under the reciprocal adequacy regimes that existed until that date. However, these gaps in the adequacy system were immediately filled on both sides:

– The Swiss FDPIC added the UK to the list of countries with adequate data protection levels, see [https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_f.pdf];

– Conversely, the UK permitted the transfer of personal data from UK to the EEA and to any countries which, as at 31 December 2020, were covered by a European Commission 'adequacy decision' (and hence to Switzerland, too), see [https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit].

Since in addition, on 28 June 2021, the EU approved adequacy decisions regarding the UK for the EU GDPR (see C(2021) 4800 final) and the Law Enforcement Directive (LED) (see C(2021) 4801 final), the largely unhindered transfer of personal data in the triangle Switzerland, UK, EU is still assured.

AI, Gatekeepers and Data Altruism: situating data protection amongst new regulatory initiatives

While many current challenges of digital regulation - and thus also issues adjacent to data protection - have been extensively discussed in the political work surrounding the drafting of the revFADP, which

has been going on for several years, substantive regulations on these adjacent matters have not yet materialised.

However, Switzerland is strongly engaged in the work of the Council of Europe and the OECD in this area, particularly with regard to the responsible use of artificial intelligence. See an overview in Jacques Beglinger, Comment la Suisse doit-elle réglementer l'intelligence artificielle?, in: La Vie économique, Plateforme de politique économique, N° 7/2021, p. 25 et seq., [https://dievolkswirtschaft.ch/content/uploads/2021/07/DV_7-2021_fr.pdf]).

Switzerland also traditionally relies on self-regulation and approaches that appeal to the self-responsibility of providers and consumers. In this context, efforts to establish ethical criteria and trust labels currently stand out. See inter alia specifically the work of the Swiss Digital Initiative, which relies on a public-private partnership for an internationally applicable Swiss Digital Trust Label (see [https://www.swiss-digital-initiative.org/digital-trust-label]).

General update: United Kingdom

Written by: Leonard Hawkes

The Impediments to the enforcement of GDPR

A response will depend on how this question is to be understood.

In one sense, it is no longer relevant: because the UK has left the EU, established its independence from the EU legal order and is to be treated as a 'third country' (outside the EU) including for GDPR purposes. The UK can now decide on its own Data Protection laws.

However, the GDPR was implemented in the UK before exit from the EU and as such falls within the class of retained EU legislation (see endnote (a)).

Moreover, there are now adequacy decisions by which, on the one hand, the UK recognizes that the GDPR is adequate from the point of view of the UK Data Protection law and, on the other hand the EU Commission has recognized that the existing UK legislation is adequate from the point of view of GDPR. (Adequacy Decision of 28 June.)

As will be seen below, the situation is not however static.

Relevant developments:

Transitional period

The UK left the EU on 31 January 2020 and it entered a post-withdrawal transition period. During the transition period (which ran until 31 December 2020), the GDPR continued to apply and it was 'business as usual' for exchanges of personal data between the EU and the UK (see endnote (b)).

Secondary legislation, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("DPPExitRegs19"), came into force on "exit day" (see endnote (c)). The DPPExitRegs19 confirm that the "UK GDPR" is the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the Withdrawal Act 2018 (see endnote (d)).

Amongst other things, the DPPExitRegs19 remove all references to the European Institutions from the DPA18 so that it becomes a purely domestic UK legislation.

The UK-EU Trade and Cooperation Agreement ("TCA")

The TCA, agreed on 24 December 2020 (and subsequently ratified by the European Parliament), set forth interim provisions for continuing the transmission of personal data from the EU to the United Kingdom initially until 1 May 2021 with an automatic extension until 1 July 2021 if there was no decision on the adequacy of the UK's data-privacy regime by 1 May (TCA Final Provisions, Article FINPROV.10A).

In the event the adequacy Decision was taken by EU Commission on 28 June 2021 (Commission Implementing Decision C(2021) 4800 final).

For the UK's approach to international data transfers see: https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers

C(2021) 4800 Article 1

1. For the purposes of Article 45 of Regulation (EU) 2016/679, the United Kingdom ensures an adequate level of protection for personal data transferred within the scope of Regulation (EU) 2016/679 from the European Union to the United Kingdom.

C(2021) 4800 Article 3

1. The Commission shall continuously monitor the application of the legal framework upon which this Decision is based, including the conditions under which onward transfers are carried out, individual rights are exercised and United Kingdom public authorities have access to data transferred on the basis of this Decision, with a view to assessing whether the United Kingdom continues to ensure an adequate level of protection within the meaning of Article 1.

C(2021) 4800 Article 3

4. Where the Commission has indications that an adequate level of protection is no longer ensured, the Commission shall inform the competent United Kingdom authorities and may suspend, repeal or amend this Decision.

C(2021) 4800 Article 4

This Decision shall expire on 27 June 2025, unless extended in accordance with the procedure referred to in Article 93(2) of Regulation (EU) 2016/679.

Potential Divergence

The UK's Department for Digital, Culture, Media & Sport (DCMS) launched "Data: A New Direction" a public consultation on its proposed reforms to the UK's data protection regime on 10 September 2021.

The consultation is 146pp long and will close on 19 November 2021.

Proposed key changes include:

- Reducing barriers to responsible innovation
- Reducing compliance burdens on businesses
- Boosting trade and reducing barriers to data flows
- Delivering better public services

 Reforming the Information Commissioner's Office (ICO)

Potential Divergence - Example: Reducing barriers to responsible innovation

Data: A New Direction - Para 48 "(…) data subjects should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purpose of personal data processing at the time of data collection. The government also proposes stating explicitly that the further use of data for research purposes is both (i) always compatible with the original purpose and (ii) lawful under Article 6(1) of the UK GDPR".

Q1.2.8. To what extent do you agree that it would benefit researchers to clarify that data subjects should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purpose of personal data processing at the time of data collection?

Comment

'What the UK GDPR is going to be in the future is what divergence makes it'.

(With apologies for the misquote to Bob Kahn - co-inventor of the TCP/IP protocols and originator of DARPA's Internet program.)

Endnotes:

(a) Section 3 of the European Union (Withdrawal) Act 2018 (the "Withdrawal Act") incorporates direct EU legislation (as defined) that was operative immediately before exit day (31 January 2020) so that it remains part of UK domestic law. As it was an operative EU regulation for this purpose the GDPR was therefore incorporated in UK domestic law by the Withdrawal Act.

(b) The UK Information Commissioner's Office issued a Statement on 29 January 2020, which said, amongst other things: "During [the transition] period, which runs until the end of December 2020, it will be business as usual for data protection".

(c) Statutory Instrument 2019 N° 419. Exit day is defined as 31 January 2020 in the European Union (Withdrawal) Act 2018 (Exit Day) (Amendment) (No. 3) Regulations 2019, Statutory Instrument 2019 N° 1423.

(d) DPPExitRegs19, Op cit, Regulation 2.