



**Ministry
of Digital Transformation
of Ukraine**



**"Analysis of Data Privacy Laws and Legislation in Ukraine"
Final Report (the "Memorandum")**

prepared by Sayenko Kharenko

14 September 2020



SAYENKO KHARENKO
NEWLAW FIRM

This Initial Report became possible due to the support of the American People through the United States Agency for International Development (USAID) under the Competitive Economy Program in Ukraine (via the Subcontract №: CEP-2020-064 for implementation of the grant activity "Analysis of Data Privacy Laws and Legislation in Ukraine"). The Initial Report and its results do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY	3
II. METHODOLOGY	4
III. FINDINGS AND ANALYSIS	5
Part One – Jurisdictions	5
Section 1. The EU General Data Protection Regulation (EU) 2016/679	5
Section 2. GDPR implementation in Germany	17
Section 3. Data privacy legislation of Israel. Privacy Protection Law (the "PPL")	18
Section 4. California Consumer Privacy Act (USA)	23
Section 5. United Kingdom. Data Protection Act of 2018 (the "DPA 2018")	27
Section 6. Turkey	30
Part Two – Specific Inquiries	33
Section 1. Data subject rights, especially, the right to be forgotten. How did governments of analysed countries contribute to the law and procedure on personal data erasure?	33
Section 2. Processing of special categories of personal data: best practices in analysed countries concerning the processing of biometric and other sensitive data	36
Section 3. Automated individual decision-making, including profiling: How this issue is regulated in legislation and practice of analysed countries	38
Section 4. Certification: do analysed countries conduct certification? Analysis of certification mechanisms, best practices. Qualification and competence of certification body if any?	39
Section 5. Direct marketing by government institutions and business: What procedures are implied in analysed countries for personal data processing for direct marketing?	42
IV. FINAL CONCLUSIONS AND RECOMMENDATIONS	46
1. Conclusions for the new UkrDPL	47
2. RTBF and other data subject rights for the new UkrDPL	51
3. Special categories of PD for the new UkrDPL	52
4. ADM prerequisites for the new UkrDPL	52
5. Certification approach for the new UkrDPL	52
6. Direct marketing approach for the new UkrDPL	54

I. EXECUTIVE SUMMARY

The below comparison between the EU General Data Protection Regulation (the "**GDPR**") and the national laws of Germany, the UK, Israel, Turkey, and California shows that globally the GDPR as a basis of law is getting more and more global importance on a regulatory level. All compared non-EU laws (Israel, Turkey, and California) lean towards the regulations outlined in the GDPR. This has several reasons from a business perspective and to be competitive on a global level (including the prospect of an EU adequacy decision) as well as a promised potential EU membership (Turkey). The GDPR seems to become the most important standard in the Western world and has already amended the laws and business approach of the top G7 countries (including, e.g., Japan, which was also obtaining an EU adequacy decision in 2019).

Compared to the Ukrainian reality and legal environment, the Israeli and Turkish data protection amendments to comply with the EU standards can serve as a baseline. Both law regimes do not have a very longstanding history for a strong data protection legal environment, including the regulations, the case law and the regulatory enforcement activities. They are, therefore, the closest to Ukrainian reality and can also identify possible challenges and requirements that need to be fulfilled to obtain an EU adequacy decision for Ukraine.

Germany and the UK, on the other hand, have a much stronger history of data protection being regulated, enforced and taken seriously, which is also reflected by the data subjects requests and court claims filed in these two countries. However, the German and the UK examples can be helpful for identifying best practices in EU Member States¹. Germany and the UK may also be good examples for Ukrainian lawmakers in terms of existing administrative and civil case-law protecting the data subject rights in a strict and efficient manner as well in terms of having a powerful and effective national Data Protection Agency ("**DPA**")².

The Californian CCPA and the future CPRA are mainly regulating personal data ("**PD**") used for business purposes (by business and for business). However, the current draft of the CPRA also shows a lot of similarities to the GDPR (e.g., data subject rights) and the importance of European law principles, now also applicable for the US IT giants located in the Silicon Valley (e.g., Facebook, Alphabet, Amazon, Apple, Microsoft). The enforcement of the CPRA seems even more realistic after the latest European Court of Justice ("**ECJ**") court decision on the Privacy Shield's invalidity.

Therefore, the future update of the Ukrainian data privacy law ("**UkrDPL**") should be mainly based on the GDPR. However, some aspects and principles outlined in the GDPR do not seem to fit the Ukrainian reality and should not be adopted (please see below, under Chapter IV).

Besides stronger legislation, Ukraine also would need a more powerful and independent data protection authority ("**UkrDPA**")³. This authority would need to obtain several regulatory and lawmaking powers and obligations similar to the best practices and standards outlined below. In practice, the new UkrDPA must be very proactive in publishing guidelines for the most pressing data protection issues and support the Ukrainian data subjects to protect their rights from a regulatory level (e.g., as the ICO in the UK). The simple enforcement of an updated law without this aspect will probably not be sufficient to fulfil the requirements to obtain an adequacy decision from the EU Commission or to fulfil the obligations outlined in the EU-Ukraine Association Agreement. The protection of data privacy rights needs to be practically enforced, and the awareness for data privacy needs to be increased by a higher level of penalisation, enforcement and practical guidance and education. As outlined below, the new UkrDPA would need to be a much more independent acting authority having similar powers to a national DPA in Europe.

Ukraine would need a new regulation concerning the establishment and provision of certain powers to its new UkrDPA. From a legal point of view, the most helpful potential examples from the assessed law regimes are the German and the UK DPAs. Although the German model foresees a split of powers based on its federation on state levels, the German laws concerning the establishment of the federal and one state DPA

¹ The UK will follow European data protection law until the end of 2020 (for more details, please see below).

² Although a German example with its state DPAs may not be the right choice for Ukraine being a non-federal country.

³ This seems one of the core requirements that need to be fulfilled to obtain an adequacy decision from the EU Commission.

can support as a baseline for the Ukrainian approach to have a single DPA on a purely national level. Based on the heritage from continental law, the German law is much closer to Ukrainian law, than the UK law.

The current fines are more an invitation to disregard the law instead of an effective mechanism to force Ukrainian data controllers and processors to comply with the current UkrDPL. However, we suggest not to uplift the potential penalties to GDPR level (e.g., Germany foresees an administrative fine of up to EUR 50,000).

As a separate enforcement matter, we suggest introducing a robust damage compensation mechanism for data subjects, and especially for groups of data subjects. Although class actions are not a familiar option of damage compensation in Ukraine, it is one of the core requirements for positive adequacy decisions by the EU Commission. The collective representation approach in the form of class actions will also be further harmonised within EU Member States legal frameworks in the coming years⁴, including the collective redress for data protection violations⁵.

For most of the specifically identified topics outlined in Part Two (right to be forgotten, sensitive data, automated making processes, direct marketing), we suggest to fully comply with the GDPR standards and to implement the same in Ukrainian law⁶.

Adoption of the main principles and concepts of the GDPR in UkrDPL would be challenging for Ukrainian businesses in the same way as it is burdensome for European businesses (please see below, under Part One, Section 1., 3.). However, the relationship with European and other Western customers practically already forces Ukrainian businesses to get compliant with the GDPR and other EU regulations. Ukrainian business acting with personal data on an international level already started adopting the GDPR standards internally, even in Ukraine. The driving force is not only the potential penalty fines for Ukrainian companies falling in the scope of the GDPR⁷ but to stay competitive for European and other Western clients on a global market.

II. METHODOLOGY

The methodology applied to the Memorandum was tailored to the RfP of Chemonics International Inc (the "**Client**") as the client and the Technical Proposal prepared by Sayenko Kharenko and adjusted at the request of the Client as per the meeting on 14 July 2020.

Having an understanding that the ultimate purpose of the Project is to provide Verkhovna Rada's Data Privacy Working Group (the "**Working Group**") with a detailed analysis of best practices in data privacy for the future amendment of the legislation pursuant to the commitment with the EU to implement the regulations of the GDPR into national legislation, we have assessed and deliver below:

- the main provisions of the GDPR;
- peculiarities of the data protection regime in those jurisdictions indicated by the Client (Germany, the UK, Turkey, Israel and California, USA);
- specific data protection issues indicated by the Client (e.g., direct marketing, automated decision making, sensitive data processing, the data subject rights and certification);
- the main aspects for a positive EU adequacy decision for Ukraine; and
- an overall conclusion about the question of how the future Ukrainian data privacy law should be established and enforced.

Considering the approach of the EU Commission to assess the level of data protection in a third country by application of the adequacy decisions criteria (Article 45, GDPR), the assessment of data protection regime in the indicated jurisdictions was conducted also from the perspective of these adequacy criteria. This included, *inter alia*, the assessment of the 29WP opinions issued for the adequacy decisions (e.g., Opinion

⁴ On 30 June 2020, the EU Commission proposed a [Directive on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC](#).

⁵ Data protection violations usually affect a whole class of data subjects involved in processing, and, thus, the individual claim approach complicates a fair judicial redress.

⁶ Mainly for reasons of legal security and higher global competitiveness of Ukrainian service providers.

⁷ By, e.g., offering services and goods to or monitoring the behaviour of data subjects when physically located in the EU (Article 3(2), GDPR).

of the Israel adequacy decision⁸), the 29WP guidelines for adequacy decisions, the ECJ and ECHR case-law objecting the adequacy of the data protection provided on the grounds of adequacy decisions (e.g., the Schrems case⁹).

In the case of each jurisdiction assessed, the following issues were disclosed:

- prerequisites of the local data protection regime;
- main provisions of the local data protection regime;
- impact of the local data protection legislation on the business and society;
- oversight and supervising authorities in the jurisdiction, their role and function; and
- pros and cons of the local data protection regime in the view of recognition of its adequacy level by the EU Commission and the practices to be considered when amending the UkrDPL.

The aforementioned assessment stages were supported by local and international case-law elucidating not only the enforcement of data subject rights, but also how effective, convenient and fair the particular data protection regime is, and how it addresses the principles of data protection established in the GDPR.

Having an understanding, that certain jurisdictions are very specific and require a deep understanding of the local regulations or are inaccessible (e.g., the Israeli legislation is published in Hebrew), we have included several local counsels to confirm and comment on our assessment (USA, Israel, and the UK)¹⁰.

Additional specific data protection issues indicated by the Client were assessed with consideration of all jurisdictions indicated.

The conclusion and the recommendation section includes our practical suggestions on the approach to the draft of the data protection law that should be considered by the Working Group. Each recommendation is based on the conclusions provided in all sections of the Memorandum.

Based on the defined scope for this Memorandum, we were explicitly asked not to comment and assess the current Ukrainian law regarding possible gaps and necessities that need to be addressed to comply with European law and not to draft any wording for the new UkrDPL. Therefore, we only included general comments and recommendations in this regard.

III. FINDINGS AND ANALYSIS

Part One – Jurisdictions

Section 1. The EU General Data Protection Regulation (EU) 2016/679

1. What were the pre-requisites for creating the law?

Already after 2000, the European Data Protection Directive 95/46/EC (the "**Directive**") could not cope with several new challenges introduced by a growing field of new technology. The PD of data subjects ("**DS**") was not only used for the needs of business relations. More and more data processing activities and uncertainties raised within the field of social media, which made a new approach to data protection inevitable.

Before the GDPR was established, all EU and EEA Member States implemented the Directive into their national law with a huge difference in scope. This led to a challenge for a growing number of cross-border acting businesses and for the regulators to protect personal data on an equal EU level.

⁸ [Opinion 6/2009 on the level of protection of personal data in Israel](#) as of 2009.

⁹ The [Court of Justice of the European Union Judgment in Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximilian Schrems](#) (the "**Privacy Shield Invalidation Decision**") has recognised in paragraph 201 the Privacy Shield Decision invalid. Currently, the adequacy of data transfers protection to the U.S. is under assessment of the EDPB.

¹⁰ Foreign national data protection legislation was assessed on the grounds of publicly available resources (e.g., unofficial translation of the legislation, web-resources of local authorities). Furtherly, the piles of assessment requiring additional approval were provided for the analysis to local legal counsels.

On 7 December 2000, the EU Charter of Fundamental Rights (the "**EU Charter**") was enforced. It foresees in its Article 8¹¹ PD protection as a human right¹². The Charter PD principles were also reflected in the Treaty of Lisbon dated 13 December 2009¹³. On 4 November 2010, the European Commission set out a strategy to strengthen data protection regulations on a European level¹⁴. In January 2012, the European Commission confirmed the comprehensive reform plan of the Directive to be changed into an EU regulation imposing the same set of rules across the entire EU¹⁵. In 2012, the Article 29 Working Party ("**29WP**") published two opinions concerning this reform plan¹⁶.

The GDPR was drafted over a longer period of time by the European Commission, the European Parliament and the EU Council and published in the Official Journal of the European Union in April 2016, two years before its enforcement on 25 May 2018.

2. What are the main provisions of the GDPR?

The GDPR consists of 11 chapters. It contains a quite large foreword in form of recitals, which mainly reflect the lawmaker's reasoning and the balance between personal freedom and the protection of other's privacy rights.

2.1. General provisions (Articles 1-4 of the GDPR)

a) *Subject-matter, objectives, and material scope*

The GDPR aims to protect the framework for PD protection outlined in the EU Charter and the TFEU¹⁷.

The GDPR material scope applies to automated and non-automated data processing except for the EU institutions that are governed by a separate regulation. The applicability of the GDPR has several reasonable exemptions: criminal prosecution procedures, TFEU security provisions, the scope of data processing is out of EU law scope, and purely PD processing by natural persons on a pure private level ("private purpose processing")¹⁸.

b) *Territorial scope*

The GDPR applies to the processing of data processing activities on the grounds of (1) establishment, (2) targeting, and (3) application of EU law based on international law¹⁹:

- (1) the controller and processor established and operating (including storage of the data) within the EU or the state applying GDPR by virtue of law;
- (2) data processing of EU natural persons data, while offering services and goods to the naturals located within the EU regardless of their citizenship; and the monitoring of their behaviour while in the EU²⁰; and
- (3) Member State law applies by virtue of public international law²¹.

¹¹ [Charter of Fundamental Rights of The European Union 2012/C 326/02 \(Article 8\)](#).

¹² E.g., data processing must be fair; everyone has the right to access and rectify PD.

¹³ The privacy ideas were reflected in Article 16(1) in which everyone has the right of its PD to be protected. Article 16(2) ensures that all European Union institutions must protect individuals when processing PD.

¹⁴ [EU Press release as of 4 November 2010 "European Commission sets out strategy to strengthen EU data protection rules"](#).

¹⁵ [EU Press release as of 25 January 2012 "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses"](#).

¹⁶ [WP 29 Opinion 01/2012 on the data protection reform proposals](#) and [29WP Opinion 08/2012 providing further input on the data protection reform discussions](#).

¹⁷ [Treaty on European Union and the Treaty on the Functioning of the European Union](#).

¹⁸ Article 2 (2)(c) of the [GDPR](#).

¹⁹ [EDPB Guidelines 3/2018 on the territorial scope of the GDPR](#) as of 12 November 2019.

²⁰ Article 3(2) of the GDPR provides that "this Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union". Therefore, e.g., if Ukrainian companies offer services and goods to DS located in the EU (this can also be Ukrainian citizens being on vacation in the EU), and they process PD, they fall into the scope of the GDPR.

²¹ E.g., a consulate or cruiseship under EU member state flag.

The ECJ already developed case-law supporting the application of GDPR for companies located outside the EU²².

c) Definitions

In comparison to the Directive, the GDPR in its Article 4 introduces improved definitions providing more certainty to several areas newly introduced. The eight previous definitions outlined in the Directive were not changed much. However, additional 18 definitions were newly introduced²³.

2.2. Principles (Articles 5-11 of the GDPR)

According to the main GDPR principles personal data shall be:

- (a) processed lawfully²⁴, fairly and transparently ("lawfulness, fairness and transparency");
- (b) collected for specified, explicit and legitimate purposes ("purpose limitation");
- (c) adequate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimisation");
- (d) processed accurately ("accuracy");
- (e) kept in a form which permits identification of data subjects for no longer than necessary for the processing purposes ("storage limitation"); and
- (f) processed in a manner that ensures appropriate security of the personal data ("integrity and confidentiality").

Some of the GDPR principles were developed and improved on the grounds of ECHR case-law²⁵.

Consent

The principles chapter governs major conditions for the DS's consent: (i) ability of the controller to demonstrate the DS's consent; (ii) necessary clear and plain language of the consent (if in writing); (iii) right to withdraw from the consent in the manner it was provided (or easier) and (iv) informed consent provision²⁶.

The consent provision and request are governed at the possible extent, covering necessary protection in cases when the data controller's and data subjects' positions are vertical (e.g., employer-employee), obliging to disclose the precise purpose of the consented processing activities. The GDPR outlines specifically the affirmative characteristic of consent as a statement ("opt-in") and the way it should be requested (e.g., cookies approach²⁷). The data controllers are allowed processing the data within the initial consent only if such consent including the notification of the DS covers all conducted processing activities.

The EDPB²⁸ constantly develops guidelines advising on the peculiarities of consent as a legal ground for data processing under the GDPR²⁹. The most recent guidelines clarify such sophisticated issues as the validity of consent provided through the "cookie wall" and if the "scrolling" of the digital consent form can satisfy the requirement of clear and affirmative action.

2.3. Data subject's rights (Articles 12-23 of the GDPR)

²² ECJ case - [Weltimmo v NAIH \(C-230/14\)](#).

²³ E.g., the definition of profiling, pseudonymisation, health data, genetic data, biometric data, personal data breach, representative.

²⁴ Pursuant to para. 123 of EDPB "[Guidelines 05/2020 on consent under Regulation 2016/679](#)" there should be a single legal ground for data processing – "the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis, which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is."

²⁵ E.g., the "reasonable retention period" requirement – the retention period should be limited within the purpose for data processing (excluding the legitimate public interest).

²⁶ Articles 5-11, GDPR.

²⁷ ECJ case - [Case C-673/17](#) – the ECJ outlined:

- consent for cookies cannot be lawfully established through the use of pre-ticked boxes; and
- any consent obtained regarding cookies cannot be sufficiently informed in compliance with applicable law if the user cannot reasonably comprehend how the cookies employed on a given website will function.

²⁸ European Data Protection Board.

²⁹ [Guidelines 05/2020 on consent under Regulation 2016/679](#) as of 4 May 2020 (EDPB). According to the preface, the Guidelines are updated even for minor amendment reason.

The DS's rights established in the GDPR sufficiently improved in terms of their practical enforceability³⁰. The DS's rights chapter is structured in the following sections covering the following groups of rights³¹:

- transparency and modalities;
- information and access to personal data:
 - right to information (Articles 13,14);
 - right to access (Article 15);
- rectification and erasure:
 - right to rectification (Article 16);
 - right to erasure ("right to be forgotten") (Article 17);
 - right to restriction of processing (Article 18);
 - right to data portability (Article 20);
- rights to object automated individual decision-making (Article 21); and
- restrictions (derogations) to processing activities.

The GDPR has a more transparent approach of obligations for data controllers, obliging them to provide full disclosure of all data processing activities, their purpose and legal bases³².

According to Article 23 of the GDPR, each EU Member State may apply restrictions to the DS's rights to safeguard their public or vital private interest in the allowed scope³³.

2.4. Controller and processor (Articles 24-43 of the GDPR)

One of the main new concepts of the GDPR compared to the Directive is the elevated liability of the data processors. The newly introduced concepts foresee a joint responsibility of both the controller and processor of the data³⁴. The GDPR outlines in detail the relationship and respective obligations between the processing parties and introduces several additional new obligations for data controllers and processors³⁵. One newly introduced concept is the necessary content of the required data processing contract between the data controller and the processor, including obligations of the processor to also verify the instructions of the controller with included sub-processors (Article 28 of the GDPR). The GDPR now includes a practical checklist for all processing contracts and ensures that these contracts include all necessary safeguarding obligations and requirements defined between the contractual parties.

The GDPR requires for the controller and processor, in the same way, the appointment of a Data Protection Officer³⁶ and an EU Representative³⁷, if necessary.

³⁰ In the majority of the cases, the data subject can file its request directly to the processor or controller of its data.

³¹ Articles 12-23, GDPR.

³² E.g., all DS requests must be handled free of charge (with exceptions); DS must be notified about the outcome of the request; a general 30-days deadline to reply a DS request, which can be limited to 72 hours in certain cases of elevated risks for the DS. Articles 15, 28 (3)(e) of the GDPR, outlines further obligations for internal management of DS requests.

³³ The restrictions may be applied to reconcile the following legitimate reasons:

- national security;
- defense;
- public security;
- the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- the protection of judicial independence and judicial proceedings;
- the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);
- the protection of the data subject or the rights and freedoms of others; and
- the enforcement of civil law claims.

³⁴ Under the Directive, mainly the data controllers were liable for not safeguarding personal data appropriately.

³⁵ Records of processing activities, data mapping obligations, security of processing, notification obligations towards DSs and DPAs, contractual content requirements, data protection impact assessment, position of a data protection officer, position of an EU representative, code of conduct approval and certifications of the processing companies.

³⁶ Articles 37 and 38 of the GDPR.

³⁷ Article 27 of the GDPR.

The controller and processors have certain obligations and possible short deadlines (72 hours and "without undue delay") concerning new notification obligations towards the respective authorities and the data subject (Articles 33 and 34 of the GDPR) in case of a severe data breach incident.

The newly introduced concept of data protection by design and default is introduced as a direct obligation of the controller (Article 25 of the GDPR), but indirectly also affects and needs to be obeyed by the processor³⁸. The included processors are further obliged to fulfil certain obligations, when including sub-processors (Articles 28 and 29 of the GDPR).

The novum of a data protection impact assessment ("**DPIA**") is required from the data controller in cases of potentially high risk to the rights and freedoms of the data subject. If required, the controller even needs to consult with the competent DPA before processing the data (Articles 35 and 36 of the GDPR).

Overall, the GDPR outlines in a very detailed form the obligations and requirements that need to be set between all processing parties from the beginning to the end of the processing activities to safeguard the processed personal data in the most secure way. It includes all possible ways of safeguarding measures, which have proven to be practical and reasonable³⁹.

2.5. Cross-border transfers (Articles 44-50 of the GDPR)

The cross-border data transfer is another core peculiarity of the GDPR, outlining new instruments and legal bases for this area. The GDPR allows the following cross-border data transfers:

- (1) to EEA jurisdictions;
- (2) to a jurisdiction positively assessed by an EU Commission adequacy decision;
- (3) outside (1) and (2) to the recipient in the third jurisdiction under the conditions of appropriate safeguards (e.g., Model Clauses, Binding Corporate Rules ("**BCR**"), certification, Code of Conduct); or
- (4) under specific legal bases (e.g., explicit consent).

a) Adequacy Decisions⁴⁰

b) Legal Bases

Allowed legal bases for cross-border transfer are the following: (i) explicit consent with possible data transfer risks indication; (ii) contractual and pre-contractual performance; (iii) public interest or vital interest of the natural person, including legal matters (judicial defence); and (iv) the source of data is publicly available according to the EU and/or EU members legislation.

c) Safeguarding Measures⁴¹

2.6. Independent supervising authority (Articles 51-59 of the GDPR, reflected below)

2.7. Cooperation and consistency (Articles 60-76 of the GDPR)⁴²

2.8. Remedies, liability and penalties (Articles 77-84 of the GDPR)

The GDPR allows a claim to any national DPA in the EU considering the rules indicating the lead DPA for the implicating controller/processor (the "one-stop-shop rule"). Any injured natural person can file a claim to any DPA without the risk of rejection due to procedural failure (e.g., inapplicable DPA).

³⁸ Article 28 foresees that the controller must only include processors into the processing activities having implemented adequate measures meeting the requirements of the GDPR (Article 28(1) of the GDPR).

³⁹ E.g., contracts between all processing companies, technical and organisational measures of each processing company by design and default, instruction line mainly governed by the data controller, consultations with DPAs if necessary, notifications of authorities and data subjects in severe incidents.

⁴⁰ For more detail please see below under chapter 5.

⁴¹ For more detail please see below under chapter 5.

⁴² This Chapter of the GDPR governs issues of cooperation between the DPA's of the member-states bound by the GDPR on the grounds of consistent GDPR application (Article 63), EDPB competences (Article 70) and composition (Article 68).

The GDPR introduces the rule that each controller or processor shall be held liable for the entire damage caused by their fault for the effective compensation. The fine range for GDPR violations (e.g., for simple non-compliance) can reach up to EUR 20 million or up to 4 % of the violator's worldwide turnover. The DS can turn to both processor and controller for damage compensation at the same time.

2.9. Provisions relating to specific processing situations (Articles 85-91 of the GDPR)⁴³

2.10. Delegated acts and implementing acts (Articles 92-93 of the GDPR)⁴⁴

2.11. Final provisions (Articles 94-99 of the GDPR)⁴⁵

3. What is the outcome, and/or impact of the GDPR on business and society?

The GDPR is complicated in procedures. The business, non-commercial organisations, state-owned organisations are required in practice to establish a separate organisational stream for data processing in order to fulfil the adequate level of organisational and technical measures under the GDPR.

The data processing professionals (e.g., IT/tech sphere, web-search engines) engaged in international data transfers have to develop their procedures and products dynamically, considering a regular risk assessment, and foresee potential consequences before evolving.

Overall, companies struggle to comply with the GDPR due to still existing uncertainties (e.g., what data protection – by default and design – is necessary in the individual case) and the detailed obligations for all processing parties. The GDPR will be a business challenge for the next decades ahead. However, for all companies who want to stay competitive on an international market, it is better to overfulfil the requirements of the GDPR and not to overlook main obligations. It is not expected that the EU will soften the obligations' level for controllers and processors established in the GDPR.

Official reports of EU institutions

According to EU Commission Communication to the European Parliament and the Council⁴⁶, the GDPR obligations are considered to be burdensome and challenging for small and medium-sized enterprises (the "SMEs")⁴⁷.

According to the EU Council⁴⁸, the SMEs should be provided with further guidance and supported by the national supervisory authority. The local DPA should develop practical tools (unified notification forms, applications, etc.), provide a simple processing record approach and legal assistance to facilitate the GDPR implementation for the SMEs.

GDPR case-law

Under the GDPR controllers and processors bear liability not only for data breaches but also solely for any non-compliance with GDPR standards. Two of the top-5 biggest fines in the GDPR history were imposed for simple non-compliance with the GDPR:

- in the "Google LLC case", the French DPA (CNIL) triggered by private claimants (data subjects) imposed a fine in the amount of EUR 50 million for the failure to comply with the obligation of

⁴³ Chapter 9 of the GDPR governs a number of specific rules related to specific processing situations: (i) obligation of reconciliation of the "freedom of expression" (Article 85) and "public access to official documents by authorities" (Article 86) to the right to the protection of personal data, including by way of derogation from a number of GDPR provisions; (ii) leverage for producing specific rules and conditions ensuring DS's rights in employment-related processing (Article 88), processing of the national ID (Article 87), and reconciliation of the secrecy to the data protection rights (Article 90); (iii) opportunity for derogations from a number of GDPR provisions for the purpose of "public interest" processing; and (iv) application of GDPR to data processing by religious organisations.

⁴⁴ Provisions of Chapter 10 of the GDPR describes the procedure of awarding the EU Commission with the ability to develop standardised icons and imagery to be used to communication information as well as develop GDPR certification mechanisms.

⁴⁵ The Final provisions of GDPR elaborate issues of GDPR validation, coming in force and the repeal of the Directive.

⁴⁶ [Communication From The Commission To The European Parliament And The Council](#) - Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation as of 24 June 2020.

⁴⁷ E.g., accountability and recording provisions of the GDPR are complicated in implementing by the SMEs due to the lack of support and guidance from the respective authorities; some GDPR obligations that are reasonable for professional data organisations or large-size enterprises are not clearly exempted for SMEs (e.g., same necessity to fulfill recording obligation for companies with less than 250 employees).

⁴⁸ [Council position and findings on the application of the GDPR as of 15 January 2020.](#)

transparency and information, and for the failure to obtain a valid legal ground for data processing. The "Google LLC case" is the largest GDPR fine imposed so far; and

- in the "Deutsche Wohnen SE case"⁴⁹ the German DPA imposed a fine in the amount of EUR 14.5 million for the failure to establish a data storage system allowing to erase the data that was no longer necessary. Such a significant fine was rather a settlement (the DPA could impose up to EUR 28 million) because the violator was trying to remedy the violation, and the DPA could not prove that the violation resulted in leakage or other unauthorised disclosure. The Deutsche Wohnen SE case remains the 4th biggest fine in the GDPR history⁵⁰.

The ECJ case law also reflects a further development based on the strong enforcement of the GDPR, including the below examples.

- The "private purpose processing" exemption application for data processing under the GDPR was supported by the ECJ in *Ryneš* (Case C-212/13)⁵¹ within the existence of the Directive. Such a "private purpose processing" cannot include in collateral processing of data which is subject to the GDPR. Controllers and processors cannot misuse the exemption for their professional purpose (e.g., internet providers).
- The spread of the territorial scope of the GDPR was clarified by the ECJ as well⁵². The ECJ stated that the requirement of global de-listing of data in terms of the "right to be forgotten" (the "**RTBF**") (e.g., URL reference for search engines applied from any country in the world covered by such a search system) cannot be justified by reference to the GDPR. However, the RTBF applies to the EU Member States and in such a way requires the data controllers and processors to apply criteria for correct fulfilment⁵³.
- The Schrems ECJ case⁵⁴ qualifies the assessment of adequacy decisions (Safe Harbor U.S., and U.S. Privacy Shield adequacy decisions) and protects data transfer to third countries articulated therein.

4. What are the regulatory and oversight bodies under the GDPR?

The GDPR establishes a strong and independent role of competent DPAs of EU Member States on a national level and the role of the EDPB and the European Data Protection Supervisor ("**EDPS**") on a European level.

a) Enforcement and supervision by DPAs

Each Member State has its own DPA⁵⁵. According to Article 58 of the GDPR⁵⁶, the DPAs have both administrative and enforcement powers. Moreover, the DPAs are independent authorities and they "remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody"⁵⁷. The independence of the DPAs can be challenged in court⁵⁸.

The national DPA members:

- should be appointed through transparent procedures (Article 53(1)) by:
 - the parliament;
 - the government;
 - the head of the State; or

⁴⁹ "[Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft](#)" (die Deutsche Wohnen SE) 5 November 2019.

⁵⁰ Top 5 biggest GDPR fines: (i) [Google](#) – EUR 50 million (imposed by French CNIL); (ii) Italian telcompany [TIM](#) – EUR 27.8 million (imposed by Italian Garante); (iii) [Österreichische Post AG](#) – EUR 18 million (imposed by the Austrian Data Protection Authority); (iv) [Deutsche Wohnen SE](#) – EUR 14.5 million (imposed by German Datenschutzbeauftragte); and (v) German [1&1 Telecom GmbH](#) – EUR 9.55 million (imposed by German Datenschutzbeauftragte).

⁵¹ [Ryneš](#) (Case C-212/13) – ECJ precedent clarifying the application of private purpose data processing to collateral non-authorised data processing.

⁵² [Case C-507/17 Google v CNIL](#) – ECJ precedent clarifying application of the "right to be forgotten" within the territorial scope EU Directive.

⁵³ According to the court findings, the data controllers and processors should obey the following rules when applying the RTBF ([Case C-507/17 Google v CNIL](#)):

- they must limit the information disclosure applying the geolocation criteria (e.g., requests from EU member-states); and
- reconcile a right of free access to information for third countries (not subject to the GDPR) and the "right to be forgotten" at the same time.

⁵⁴ [Case C-362/14 Maximilian Schrems v Data Protection Commissioner](#) – ECJ case resulted in invalidation the Privacy Shield adequacy decision.

⁵⁵ E.g., Commission Nationale de l'Informatique et des Libertés (CNIL) in France, Information Commissioner's Office in the UK (the "**ICO**") and Agencia Española de Protección de Datos (AEPD) in Spain.

⁵⁶ [GDPR Article 58](#).

⁵⁷ [GDPR Article 52 \(2\)](#).

⁵⁸ [European Commission v. Republic of Austria \[2012\] C-614/10](#), 16 October 2012 and [C-518/07 Commission v Germany \[2010\] ECR I](#).

-
- entrusted for appointment independent authority.
 - have necessary qualifications, experience and skills, particularly in data protection (Article 63(2));
 - will hold the membership within the expiring period of four years (Article 54 (1)(d));
 - can be dismissed before the expiration period only due to the serious misconduct;
 - shall be provided with independence by means of remaining free from external influence (Article 52 (2));
 - shall not combine professional functions as a DPA member with any incompatible duties and/or remain engaged in any incompatible occupation regardless of its profitability (Article 52 (3)); and
 - shall be limited in actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment in the DPA (Article 54 (1)(f)).

From the organisational perspective, the national DPA as an authority (governmental body):

- shall be provided with enough human, technical and financial resources, premises and infrastructure necessary for the performance of tasks and exercising the powers (Article 52(4));
- shall have freedom of own staff choosing which shall be subject to the exclusive direction of the DPA (Article 52 (2));
- shall be subject to financial control which does not affect its independence and that it has separate, public annual budgets (Article 52 (6));
- shall be provided by the State with the eligibility criteria for the membership and the relevant procedures for getting admission (Article 54 (1)(c)(d));
- shall be limited in the terms of reappointment (Article 54(e)).

The competent DPAs have, e.g., the following tasks and powers:

- development of national law: each DPA is entitled with the powers to provide guidelines and recommendations concerning the interpretation of EU and national law (e.g., ICO guidelines⁵⁹);
- promote awareness among data subjects: in 2019, still, only 57% of the data subjects in the EU were aware of the existence of the authority responsible for data protection⁶⁰;
- investigative powers (Article 58(1)): DPAs' rights are very broad and give them all powers to audit and investigate both controllers and processors;
- corrective powers (Article 58(2)): DPAs cover the full range of options, including a ban on processing, shut down of servers and imposing administrative fines. All mentioned powers can cause severe consequences on businesses;
- authorisation and advisory powers (Article 58(3)): DPAs' rights and obligations in the sphere of assessing and confirming codes of conduct, certifications, marks and seals and international transfers of PD; and
- initiating legal proceedings (Article 58(5)): each DPA must have the power to bring GDPR infringements before courts.

Based on the European best practices concerning the establishment and structure of a national DPA as outlined above, and based on the potentially aimed application of Ukraine for an EU Commission adequacy decision, we suggest to implement the above outlined standards also into Ukrainian law and to provide the new Ukrainian DPA with similar powers and tasks than the national DPAs in the EU Member States. The GDPR should be a guideline for Ukrainian lawmakers in terms of law wording and structure.

b) European Data Protection Board

The EDPB is an independent European body, which was established based on Article 68 of the GDPR. However, it is not a newly established body it is the successor of the 29WP in a new format. The EDPB should act independently and has a row of new obligations (Articles 69 and 70 of the GDPR). Among others, it has the obligation to ensure the consistent application of the GDPR and to promote good cooperation

⁵⁹ [Guide to Data Protection](#) issued by Information Commissioner's Office.

⁶⁰ [Infographic "GDPR in figures"](#).

among all DPAs in the EU. The EDPB can publish opinions, guidelines and recommendations⁶¹ for controllers/processors and individuals (Article 64(1) of the GDPR).

⁶¹ [Link to EDPB web-site page with published EDPB and endorsed WP2929WP guidelines.](#)

c) *European Data Protection Supervisor*

The EDPS was established based on the Regulation (EC) No 45/2001⁶², which is now being updated to be in line with the GDPR. The EDPS' main function is ensuring compliance with the GDPR by European authorities⁶³. Moreover, the EDPS is working closely with the EDPB and cooperates with all EU DPAs. The EDPS has also the powers to represent the EU in ECJ proceedings and proceedings before the General Court.

5. What are the requirements for the standards for international data transfers?

According to Chapter V of the GDPR, there are several legal grounds based on which a data transfer from the EU to non-EU countries is allowed (please see above, under 2.5.).

a) *Adequacy decision*

One of the most convenient approaches for a non-EU state for free data transfers from the EU is obtaining an EU Commission adequacy decision. Data transfers to a non-EU state having such adequacy decision do not require any additional legal bases (Article 45(1) of the GDPR). The procedure and the requirements for adequacy decisions are qualified and represented in the EU Adequacy Referential⁶⁴ and the recent adequacy decision for Japan⁶⁵. Adequacy decisions are considered to be a valid ground for cross-border transfer during 4 years after granted and/or successfully reviewed, or not challenged within the ECJ case-law (e.g., Safe Harbor decision in Scherms case⁶⁶).

In practice, the EU Commission awards adequacy decisions on the grounds of an opinion issued by the EDPB in accordance with Article 70 (1)(s) of the GDPR and Articles 2 and 12 of the European Data Protection Board Rules of Procedure⁶⁷. Previously, this was a function of the 29WP. The 29WP has prepared 12 opinions for adequacy decisions. Prior to first adequacy decisions, in 1998, the 29WP has issued a Working Party document WP12⁶⁸ covering all the key questions for an adequacy decision. Although the 29WP was replaced by the EDPB (Article 94 (2) of the GDPR), the WP12 remains a solid step-plan for the assessment of the adequacy of protection provided by the third country.

The current requirements for an adequacy decision are set out in more detail in Article 45(2) of the GDPR and can be summarised as follows:

- (a) legislation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- (b) the existence and effective functioning of independent supervisory authorities ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- (c) the international commitments the third country concerned, in particular in relation to the protection of personal data.

The EDPB and the EU Commission evaluation also includes the following:

- proper legal regime for data protection and rule of law in broad meaning (including other international commitments, e.g., the EEA);
- data subject's access to effective enforcement and judicial proceedings;
- independent, powerful and efficient supervising authority;
- the ECJ and ECHR case law related to data privacy issues;

⁶² [Regulation \(EC\) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.](#)

⁶³ [Link to EDPS web-site page with indication of EDPS role and functions.](#)

⁶⁴ [EU Adequacy Referential \(2008\).](#)

⁶⁵ [EU-Japan Adequacy decision \(2020\).](#)

⁶⁶ ECJ case – [Data Protection Commissioner vs Schrems, Facebook \(Case C-311/18\).](#)

⁶⁷ [European Data Protection Board Rules of Procedure](#) as of 25 May 2018 (modified as of 2020) – pages 5 and 13.

⁶⁸ Working Document "Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU data protection Directive" adopted by the 29WP/29WP set up under Article 29 of the Directive on 24 July 1998.

-
- the adequacy assessment and the pertaining 29WP and EDPB guidelines (e.g., the WP12); and
 - the recent and future amendments to the GDPR (e.g., the Privacy Shield decision was adopted with the consideration of the GDPR coming in force).

The history of adequacy decisions, meanwhile, counts 13 decisions opening data flows to third countries out of the EU (12 during the validity of Directive). In five cases (Canada, Faeroe Islands, Israel, U.S., and Japan) the adequacy decisions were granted with limitations (reservations) (please refer below to Annex I for the full list of EU adequacy decisions).

The countries awarded with an adequacy decision are subject to systematic monitoring by the EDPB. Each of the adequacy decisions issued after the GDPR came in force includes the mechanism of periodic review⁶⁹.

In most recent negative assessments of jurisdictions for an adequacy decision, the EU Commission repeatedly referred to the necessity of the "independence of the supervising authority"⁷⁰.

On 16th July 2020, the ECJ for the first time in the history of EU Commission adequacy decisions invalidated the Privacy Shield Decision⁷¹. The Privacy Shield Decision invalidation settled a precedent contesting the status of the adequacy decision.

Considering the last two adequacy decisions (U.S. Privacy Shield and Japan) and the recent case-law, Ukraine as a candidate would need to establish a solid legal framework covering data protection issues within the GDPR extent and local peculiarities, represent efficient enforcement within the real case-law, establish a powerful and independent UkrDPA, proactively articulating the introduced rules to the business and society and foresee and develop the legislation towards the twists and novelties of upcoming data relations.

Transfers subject to appropriate safeguards

International data transfers from the EU to outside include strict regulations under the GDPR. The companies that are located in countries not providing an "adequate" level of data protection must find and implement an allowed mechanism to ensure an adequate protection level for the data transfer. The instruments foreseen by the GDPR so far are the following: (1) Model Clauses⁷²; (2) BCR⁷³; (3) Certification⁷⁴; and (4) Code of Conduct⁷⁵. The BCR and Certification application is complicated and takes a long time (according to our experience minimum one year). The Model Clauses or Standard Contractual Clauses (the "SCCs") can only be used for two cases (EU exporter is a controller and the importer is either a controller or processor). E.g., if the exporter is a processor and the non-EU importer is a controller (e.g., Ukrainian headquartered IT-company), the company must draft new SCCs and one of the competent EU DPAs must approve the same including the approval of the EDPB before they can be a legal basis for data transfer outside of the EU. All the aforementioned is a huge struggle for business.

b) Model Clauses

The direct use of the approved SCCs without any changes in their wording allows the export of data to outside the EU. Currently, the EU Commission has adopted three valid SCCs on the ground of the Directive:

⁶⁹ Adequacy decisions granted under the GDPR are subject to review at least each 4 years after issued, the Directive decisions are under pending monitoring (not limited). In case of discrepancies revealed, the EU Commission shall enter into consultations with such a country to remedy the inconsistency and lack of protection (Article 45(6)). If the EU Commission shall find it necessary to revoke the adequacy decision granted, the data flows ensured by other safeguards (e.g., SCCs) will not be affected, if not revoked specifically (Article 45(7)).

⁷⁰ [Answer given by Ms Jourová on behalf of the Commission](#): "The Commission recently indicated that Turkey needs to amend its legislation on personal data protection in order to ensure that it is in line with the EU acquis (notably to guarantee that its data protection authority can act in an independent manner and that the activities of law enforcement agencies fall within the scope of the law)."

⁷¹ [Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximilian Schrems](#) as of 16 July 2020 (Schrems II).

⁷² Article 46 (2)(c) of the [GDPR](#).

⁷³ Article 47 of the [GDPR](#).

⁷⁴ Article 46 (2)(f) of the [GDPR](#).

⁷⁵ Article 46 (2)(e) of the [GDPR](#).

- SCCs for the transfer of personal data to third countries in 2001 (recipient-controller) (the "**Decision 2001**")⁷⁶;
- an alternative set of SCCs for the transfer of personal data to third countries in 2004 (recipient-controller)⁷⁷; and
- SCCs for the transfer of personal data to processors established in third countries in 2010 (recipient-processor) (the "**Decision 2010**")⁷⁸.

The SCCs issued under the aged Directive remain valid until amended, replaced or repealed by the EU Commission pursuant to Article 46 (5) of the GDPR. Considering the pending overview of the protection level provided by the adequacy decision and the SCCs⁷⁹, the EU Commission amended the above-mentioned Decision 2001 and Decision 2010⁸⁰.

c) Certifications

The GDPR establishes some novelties for the EU to outside data transfers by a prior certification of the transferring parties. The Certification under Article 42 of the GDPR is a voluntary process to assist controllers and/or processors in demonstrating compliance with the GDPR. The EDPB and the national DPAs are to introduce the rules of establishing certification mechanisms. The EDPB published guidance for the certification mechanism and accreditation⁸¹. The EDPB still must adopt the certification seal. Each national DPA also has to introduce similar proceedings for certification under the GDPR.

The Luxemburg DPA is a "pioneer" that introduced the certification criteria and mechanisms⁸². The ICO was the next DPA publishing general guidance in this regard⁸³. A small number of other EU members started developing their certification schemes as well. The certification mechanism introduction is a complicated task due to the following, but not limited by, issues:

- certification should precisely name the data processing activities protected; consequently, a universal approach is not applicable;
- the criteria of certification assessment should include three components: personal data; technical requirements; data processing activities in detail; and
- certification approach can be requested by the business only if detailed and practical instructions relevant to the data processing stream and infrastructure is provided.

d) BCR (Article 47 of the GDPR)

The BCRs are a set of rules that are based on the EU standards for data protection, voluntarily prepared and used by multinational organisations. The instrument of BCRs is an easier approach for global multinational companies than to have intragroup agreements. BCRs must be approved by competent EU DPAs. Within the approval process, the applied DPA needs to forward the request of BCR also for approval to the EDPB to fulfil the consistency mechanism (Article 63 of the GDPR).

In 2003, the EU DPAs developed the concept of BCRs. The concept to use BCRs was also advised by 29WP in its Working Document WP74⁸⁴, which is still used as a guideline by DPAs for the BCR approval process.

e) Code of Conduct (Article 40 of the GDPR)

⁷⁶ [2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC \(Text with EEA relevance\) \(notified under document number C\(2001\) 1539\).](#)

⁷⁷ [2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries \(notified under document number C\(2004\) 5271\)Text with EEA relevance.](#)

⁷⁸ [2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council \(notified under document C\(2010\) 593\) \(Text with EEA relevance\).](#)

⁷⁹ [Case C-362/14 Maximilian Schrems v Data Protection Commissioner](#) – ECJ case resulted in invalidation the Privacy Shield adequacy decision.

⁸⁰ [Commission Implementing Decision \(EU\) 2016/2297 of 16 December 2016](#) amending Decisions 2001/497/EC and 2010/87/EU.

⁸¹ [Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.](#)

⁸² [GDPR - Certified Assurance Report based Processing Activities \(CARPA\) certification criteria.](#)

⁸³ [Link to ICO web-site page with guidance on certification schemes.](#)

⁸⁴ [Working Document Setting up a framework for the structure of Binding Corporate Rules as of 2008.](#)

Code of Conduct is a rulebook that can be adopted by controllers and processors in a certain field (e.g., a number of SME's) in a third country who design and implement GDPR compliant data processing activities (Article 40(2) of the GDPR). An association of controllers and processors may apply the Code of Conduct for submission to the relevant national DPA (Article 40(5) of the GDPR). If the data processing activities relate to several EU Member States such a Code of Conduct is subject to submission to the EBDP by the national DPA. Since the Code of Conduct is approved by the DPA and/or EBDP, it is considered to be an appropriate safeguard for data transfer to controllers and processors bound by the approved Code of Conduct. The EBDP has developed guidelines to articulate the GDPR requirements and the submission procedure⁸⁵.

Section 2. GDPR implementation in Germany

Germany has 16 State (Länder) DPAs and a Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für Datenschutz und Informationsfreiheit – "**BfDI**")⁸⁶, representing Germany in the European Data Protection Board. The BfDI is a supervisory authority in the meaning of Article 51, however, its supervision is limited to the entire public sector at federal level, telecommunications and postal services providers. The rest is supervised by the Länder DPAs.

To control whether all German State DPAs have a unified and harmonised procedure they meet regularly at the National Data Protection Conference⁸⁷ (Datenschutzkonferenz – "**DSK**"). The DSK is publishing guidelines, e.g., how the DPA will calculate fines pursuant to Article 83 of the GDPR⁸⁸. Each of the German State DPA is active in enforcing penalties against violators⁸⁹.

In some areas explicitly mentioned in the GDPR (so-called "open clauses") the Member States have the very limited right to define in more detail or even to foresee further exemptions to the provisions outlined in the GDPR. Local courts have to apply the higher EU standards, which legally supersede national regulations if contradictory.

The German federal data privacy law, the Bundesdatenschutzgesetz ("**BDSG**") foresees a number of areas, which are even stricter than the GDPR⁹⁰. However, the German BDSG also foresees a number of exceptions, limiting the data subject rights of the GDPR (mainly for public purposes and authorities and only for the areas allowed by the GDPR).

The information material and guidelines of state and federal authorities are quite a lot⁹¹ and updated on a regular basis. A high degree of response can also be witnessed in the number of court cases based on alleged data privacy violations before German courts⁹².

The practical impact of the GDPR-related changes was also challenging for businesses in Germany. In a statistics of September 2018, 502 German mid-sized companies (over 20 employees) stated the following main challenges with the GDPR and the updated BDSG⁹³: legal insecurity (65%), hard to estimate implementation process (63%), non-existing practical support (47%), too short time period for adoption (35%), lack of educated employees (33%), difficult technical adaptation (28%), lack of financial resources (19%) and lack of support within the company (15%).

All German states (Länder) confirm a much higher awareness of data subject rights and administrative proceedings after the implementation of the GDPR and the updated BDSG. The state commission for data protection and freedom of information of Nordrhein Westfalia in its 2020 report confirms app. 12,000

⁸⁵ [Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 of 4 June 2019.](#)

⁸⁶ [BfDI web-site.](#)

⁸⁷ [The National Data Protection Conference \(DSK\) Short Paper list.](#)

⁸⁸ [DSK Guidelines, 14 October 2019.](#)

⁸⁹ The latest infringement was done by the DPA Baden-Württemberg. The violator is a big public health insurance organisation "AOK Baden Württemberg" and the penalty fine was EUR 1,24 million for noncompliance with the implementation of appropriate technical and organisational measures ([DPA Baden-Württemberg Press release: Monetary penalty for "AOK Baden Württemberg", 30 June 2020](#)).

⁹⁰ E.g., the obligation to appoint a DPO for companies having at least 10 employees managing automated data processing activities, having processing activities which need to be based on a DPIA and/or using the data for specific commercial purposes (Article 38, BDSG).

⁹¹ E.g., [guidelines of the BfDI.](#)

⁹² E.g., [Chronology of filed BDSG violations proceedings.](#)

⁹³ [Report of the state commission for data protection and freedom of information of Nordrhein Westfalia in 2020.](#)

complaints that have been filed in 2018 and 12,500 proceedings filed in 2019 before their state DPA⁹⁴. 2,235 of these administrative proceedings were initiated due to high-risk data breaches that need to be reported to the DPA within 72 hours. The average administrative fines were between EUR 100 and 1,500⁹⁵. This trend of a higher willingness to raise data protection violations is also shown on a federal level⁹⁶. The same increase since the enforcement of the GDPR and the updated BDSG also applies to the willingness of data subjects to file a civil proceeding against companies⁹⁷.

Section 3. Data privacy legislation of Israel. Privacy Protection Law (the "PPL")

1. The Privacy Protection Law and EU commission adequacy decisions prerequisites

The overview of the Israeli legislation is divided into two parts, before and after the EU Commission decision of 31 January 2011⁹⁸ (the "**Israel Decision**").

Before the Israel Decision in 2011

The Israeli law system combines both the common law and continental law approaches. The legislation adopted by the Israeli lawmaker can be supported by case-law, which is a binding precedent, and decisions of the Supreme Court of Israel granting constitutional status to "Basic laws". From a data privacy perspective, there is the Basic Law on Human Dignity and Liberty as of 1992, which has a constitutional value in the Israeli legal system, providing that "*every person has a right to privacy and to intimacy in his life*" (S.7(a)), and adopting the concept of the valid "public interest" reservation in regard of such rights (S.8-9)⁹⁹ (the "**Basic Law**")¹⁰⁰.

In 1981, the lawmaker introduced a specific law governing data issues – the PPL, 1981¹⁰¹. The PPL is considered to be core legislation and was amended several times before the Israel Decision. One of the most significant amendments was the establishment, in 2006, of the Israeli Law, Information and Technology Authority (the "**ILITA**") as the local data protection authority and its powers, and the establishment of data processing requirements in greater detail.

Before the Israel Decision, the data relations were supplemented by specific regulations and inclusions in the sectoral laws¹⁰². The conclusion of the assessment of the Israel Decision was reflected in the "Opinion 6/2009 on the level of protection of personal data in Israel" (the "**Opinion**")¹⁰³. The 29WP was exercising the PPL from the perspective of the WP12¹⁰⁴. Above the assessment of the PPL, the 29WP was considering a "Schoffman report"¹⁰⁵, as a plan of the amendments to the PPL for the lawmaker. The "Schoffman report" was evaluating the best examples of the relevant laws abroad (EU, U.S., Australia, etc.), concluding the most favourable option to compile the best legal tools suitable for Israel. The 29WP and the EU Commission granted the Israeli decision because of the conclusion in the report requiring amendments to and specifying how to amend the PPL¹⁰⁶. In 2010, after the Opinion was released, but before the Israel Decision, the ILITA

⁹⁴ [Q&A regarding the monetary fines imposition in 2020](#).

⁹⁵ Footnote before.

⁹⁶ [Q&A regarding the monetary fines imposition in 2020](#).

⁹⁷ E.g., [Chronological review of the court proceedings in federal and local German courts regarding the BDSG and GDPR violations, 6 November 2019](#).

⁹⁸ [EU commission decision of 31 January 2011](#) pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data.

⁹⁹ [Basic Law on Human Dignity and Liberty](#) as of 1992 with amendment introduced in 1994 (unofficial translation).

¹⁰⁰ The Basic Law was introduced much later than the relevant ordinary legislation, because of the inability to introduce a constitution as a single document. However, such an introduction was rather a "filling the gap", than affecting the legal framework.

¹⁰¹ [Protection of Privacy Law 1981.pdf](#) (unofficial translation).

¹⁰² Protection of Privacy Regulations approved by the lawmaker in 2001 (the "**PPR**"), e.g., governing the cross-border data transfers;

Communications Law as of 1982; and other sectoral laws governing health, financial, and public registries issues.

¹⁰³ [Opinion 6/2009 on the level of protection of personal data in Israel](#) as of 2009.

¹⁰⁴ Working Document "[Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU data protection Directive](#)" adopted by the Working Party set up under Article 29 of the Directive on 24 July 1998.

¹⁰⁵ "[Report to the Ministry of Justice by the Committee for the Examination of Legislation relating to Databases.pdf](#)" issued by the Committee for the Examination of Legislation Relating to Databases in 2007 (the report was named after the Committee chairman Mr. Yehoshua Schoffman, Deputy Attorney General).

¹⁰⁶ The "Schoffman report" specifically introduced future amendments of the PPL in the following sections:

- Application scope;
- Definitions;
- Registration requirements;
- Inspection right;
- Cross-border transfer; etc.

has issued "A guide to data protection in Israel" basically outlining the developments of data protection and the core pieces of the regulations established¹⁰⁷.

The Israel Decision does not cover non-automated data processing. This reservation was due to the inapplicability of the PPL to the processing of personal data in non-automated databases.

¹⁰⁷ ["A guide to data protection in Israel - 2010.pdf"](#) as of 2010 by ILITA, prepared by Head of Data Protection Projects, Information Commissioner's Office, UK.

Within the last years, a number of legislation pieces covering the developed sectors of data transfer and the gaps identified by the "Schoffman report" and Israel Decision were introduced, e.g.:

- Privacy Protection (Data Security) Regulations as of 2017 (the "**Data Security Regulations**") outlining the security requirements applicable to the databases¹⁰⁸; and
- Credit Data Law as of 2016 for financial data protection.

Since the establishment of the ILITA, a number of guidelines were issued related to the right to access, labour-related data processing, surveillance, direct mailing and use of outsourcing service provider.

2. Main provisions of the PPL

Similarly to the Ukrainian data protection regime, the PPL and the supporting data protection regulations introduced by Israel are based on the aged Directive. In the view of the recent ECJ decision in case Schrems II, the Israel decision could be reviewed by the EDPB and the EU Commission within the perspective of the adequacy criteria introduced by the GDPR in Article 45. The Israel data protection professionals already invoiced a worrisome about the status of the Israel decision based on the review of the implementation within the last nine years, including the following: (i) stagnated legislation amendments in compliance with the GDPR; (ii) non-realised potential of the national DPA in enforcement; (iii) complicated legislative procedures; and (iv) disbalance of the legitimate security interest and the data subject right of privacy. Being close to Ukraine in these inconsistencies with the GDPR requirements, Israel remains a good example of the path to the adequacy decision, although, it obtained the same in times of the Directive.¹⁰⁹

a) Definition of Personal Data and Sensitive Information

The definition of personal data established in the PPL does not reflect the scope of the definition of the GDPR. Section 7 of the PPL uses the general term "information" to designate personal data, which it defines as "*data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of an individual*". However, although the definition of personal data in the PPL refers solely to certain data categories, Israeli case-law has given this legal concept a broad interpretation¹¹⁰. In addition, the elements of data protection relations are defined in the PPL out of the central position of the "database": there are a "person" and a "possessor" instead of a data subject and a processor.

Section 7 of the PPL further defines a specific category of data, "sensitive information" ("**Sensitive Information**") as follows: (i) Data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person; or (ii) Information that the Minister of Justice determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, as sensitive information.

According to Section 8(c)(2) of the PPL, any database that contains Sensitive Data should be registered in an official register maintained by the Registrar via the submission of an application by the database owner.

b) Principles

The principles of data processing are established in the content of the legislation (Basic Law and PPL). The peculiarity of the PPL is the prohibition approach of rules, they mention "what is prohibited" rather than the appropriate grounds. The Opinion and the Israel Decision outlined the adequate establishment of such principles as purpose limitation, data quality and proportionality, security, rights of access, rectification and opposition.

¹⁰⁸ "[Protection of Privacy Regulations \(Data Security\) - 2017.pdf](#)" (unofficial translation). The Data Security Regulations establish four categories of databases that vary according to data sensitivity, how data is used, the number of individuals having access to the database and the number of data subjects.

¹⁰⁹ "[Israel's outdated privacy laws jeopardize relations with EU](#)", published by Globes, Israel business news - en.globes.co.il - on 23 July 2020.

¹¹⁰ In Civil Appeal 86/89 the State of Israel v. Bank HaPo'alim, the Supreme Court held that "*the term [Personal] Information should not be interpreted in a restrictive manner*" but also in accordance with the legislative purpose of the PPL. For example, in *Civil Appeal 439/88 Database Registrar v. Ventura*, the Supreme Court held that the term "information" shall also include details such as an individual's address and telephone number, bank account number and national ID number.

c) *Territorial extent*

The PPL applies to residents of Israel, data processing within Israel and establishments processing the data of Israelis. The PPL enforcement is limited to the Israeli establishment. A foreign establishment can be subject to the PPA (as such term is defined below) enforcement in case it is represented legally in Israel.

d) *Cross-border transfers*

The PPL specifies the restrictions and conditions regarding the transfer of data from databases in Israel abroad. According to Section 1 of the PPL, the transfer abroad of data from databases in Israel shall not be allowed, unless the law of the country to which the data is intended to be transferred ensures a level of protection no lesser, *mutatis mutandis*, than the level of protection of data which ought to be provided according to Israeli law¹¹¹.

According to Section 2 of the PPL, the transfer abroad of data from databases in Israel shall be allowed even if the destination country does not guarantee an adequate level of protection pursuant to the provisions included in Section 1 of the PPR described above, if respective conditions are met, which are similar to the GDPR¹¹².

When transferring data abroad, the owner of the database shall ensure that the recipient of the data executed a written guarantee whereby the recipient undertakes to take adequate measures to ensure the privacy of the data subjects and to ensure that the data shall be transferred to no other person (Section 3 of the PPL).

e) *Consent*

The PPL defines "consent" as informed, express or implied consent. The general approach is an "opt-in" consent for the vast streams of data processing (e.g., minor exemptions in case of advertisement). Consent is required even in labour relations due to the imbalanced relations of employer-employee.

f) *Sanctions, remedies, and enforcement*

Violations of data privacy can lead to administrative, severe criminal¹¹³ and civil (tort) consequences. One of the peculiarities of the administrative fines' imposition that above the regular amount distinction for persons and establishments is the introduction of the approach of fine calculation for pending violation (e.g., amount of the fine is calculated with respect to the number of days the violation was conducted). The PPL

¹¹¹ In addition, it is stated that such country shall be considered as providing an adequate level of protection, if, according to its legislation:

- data shall be gathered and processed in a legal and fair manner;
- data shall be held, used and delivered only for the purpose for which it was received;
- data gathered shall be accurate and up to date;
- the data subject has the right of inspection and reviewing; and
- there is an obligation to implement adequate security measures to protect data in databases.

¹¹² Section 1 of the PPL:

- The data subject provided his consent for the transfer;
- It is not possible to receive the data subject's consent and the transfer is essential for the protection of the data subject's health or physical wellbeing.
- The data is transferred to a corporation that is under the control of the owner of the database from which the data is transferred, and such owner has guaranteed the protection of privacy following the transfer;
- The data is transferred based on receipt's obligation, detailed in an agreement, to comply with the conditions for the possession and use of the data applying to a database in Israel, *mutatis mutandis*;
- The data was made available to the public by legal authority;
- The transfer of data is essential to the public safety or security;
- The transfer of data is mandatory according to Israeli Law; and
- The data is transferred to a database in a country: (i) which is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data; (ii) which receives data from Member States of the European Union, under the same terms of acceptance; (iii) in relation to which the data protection registrar announced, in an announcement published in the Official Gazette ('*Reshumot*'), that it has an authority aimed for the protection of privacy, after reaching an arrangement for cooperation with the said authority.

¹¹³ Data protection offences prescribed in the PPL:

- according to Section 16 of the PPL, unauthorised disclosure of the data obtained by the possessor or its employees is subject to imprisonment for a term of five (5) years.
- according to Section 5 of the PPL, a failure to apply for the registration and to register the Database, is liable to imprisonment for a term of five (5) years.
- penalty for offenses of strict responsibility: According to Section 31A of the PPL, a person who commits any of the following (without the need to prove criminal intent or negligence), is subject to imprisonment for a term of one year: (i) manages, possesses or uses a Database in violation of the registration requirement and use of Database provisions; or (ii) provides incorrect particulars in an application for registration of a Database.

defines criminal liability for offences in violation of the PPL with sanctions from one to five years of imprisonment¹¹⁴. *Inter alia*, the class action is also possible under Israeli law.

3. Main provisions of the Data Security Regulations

The Data Security Regulations provide specific data protection obligations with respect to databases, based on their classification into four (4) categories according to different parameters, including the nature and the sensitivity of the data, the number of data subjects and the data collection purposes¹¹⁵.

The owner of a database (and the manager of the database, and in some cases the possessor of the data – as detailed in *Section 19 of the Data Security Regulations*, for ease of reference, all shall be referred to herein as "owner"), is required to comply with the obligations provided by the Data Security Regulations according to the respective category to which its database belongs¹¹⁶.

4. The impact of the PPL and the Data Security Regulations on business and society

Considering the Israeli decision and the pertaining Opinion, the business and Israeli citizens were subject to developed data protection rules for a decade already. The overall effective Israeli enforcement approach triggered data controllers and processors to obey the legislative requirements supported by the judicial precedents and explained in the published guidelines. The fulfilment of requirements is annually assessed by the PPA (as defined below) (whose former name was ILITA) during compliance audits. The awarded Israel decision opened data flows and applied GDPR approach causing a greater integration of Israeli economics to global partnerships.

5. What are the regulatory and oversight bodies under the PPL?

The ILITA, which name was changed in 2017 to the Privacy Protection Authority (the "PPA"), is a major authority for data privacy compliance and enforcement. As a division of Ministry of Justice, the PPA's functions are separated in the following streams:

- administrative enforcement – investigation and administrative sanctions imposition;
- criminal enforcement – investigation and development of the criminal investigations (and civil tort if collateral);
- other functions, such as compliance auditing, handling the database register (including sensitive data), legislation and guidance development, and international issues.

Private Litigation

Under the PPL, an act or omission in violation of the provisions of chapter two of the PPL (which includes the requirements for the registration of a database) is deemed a civil tort under the Israeli Civil Wrongs Ordinance [New Version] (*Section 31B of the PPL*). In addition, the court may order that the defendant shall pay the plaintiff statutory damages that will not exceed NIS 50,000 (subject to index differential) (*Section 29A(b) of the PPL*). As such, failure to comply with data security obligations under the PPL and the regulations promulgated pursuant thereto may be actionable as a civil tort.

¹¹⁴ The PPA's most important enforcement action over the past years concerns a massive data breach involving the loss and eventual posting on the Internet of Israel's entire population registry consisting of more than 9 million records related to Israeli citizens and residents, as well as those recently deceased. The investigation resulted in criminal indictments of government contractors as well as recipients of the data, some of whom were sentenced for up to 12 months in jail.

¹¹⁵ Types of databases according to the Data Security Regulations:

- database managed by an individual;
- database subject to a basic level of security;
- database subject to a medium level of security; and
- databases subject to a high level of security.

¹¹⁶ For further information regarding the specific obligations applying to each of the 4 categories of databases, please see the unofficial translation of the Data Security Regulations ([Protection of Privacy Regulations \(Data Security\) - 2017.pdf](#)).

Data subjects have brought several class-action lawsuits, including against Apple for geolocation tracking, mobile operator Pelephone for retention of SMS content, Sony Corporation¹¹⁷ and triggered an investigation by the DPA against Facebook for processing the data above the consented purpose¹¹⁸.

Section 4. California Consumer Privacy Act (USA)

1. What were the pre-requisites for creating the CCPA?

The United States does not have an overarching privacy law at the federal level. Instead, there are numerous sources of privacy law, including laws and regulations at the federal, state, and local levels. These laws are often federal laws that only govern particular sectors and industries (e.g., Health Insurance Portability and Accountability Act (HIPAA)¹¹⁹, Children's Online Privacy Protection Act (COPPA)¹²⁰, Gramm-Leach-Bliley Act (GLBA)¹²¹, and Driver's Privacy Protection Act¹²²). Each state also governs data privacy individually on a state level through, for example, state-specific breach notification laws.

The CCPA was signed into law on June 28, 2018. During 2018-2019 various companies and industry groups (e.g., tech giants like Facebook and Alphabet), as well as privacy advocates lobbied for changes to the law. As a result, there were five amendments signed by Governor Newsom on October 11, 2019¹²³. On January 1, 2020, the CCPA became effective. Enforcement of the statute by the California Attorney General's (AG) Office began on July 1, 2020.

The CCPA became the first comprehensive state data protection law in the U.S. It prompted organisations to shift their privacy practices and served as an influence and model for other proposed state laws¹²⁴.

2. What are the main provisions of the CCPA?

The CCPA applies broadly to businesses that collect personal information about California residents and provides broad consumer privacy rights. In doing so, this law has created significant new obligations for businesses. It supplements several other privacy-related California laws, including the "Shine the Light" Law¹²⁵, the California Electronic Communications Privacy Act of 2015 (governing law enforcement's ability to obtain information)¹²⁶ and the California Online Privacy Protection Act of 2003 (CalOPPA)¹²⁷, among others.

Parts of the CCPA are comparable to the GDPR¹²⁸ but apply only for organisations doing business in California and for California residents.

a) Definitions

The CCPA outlines major subjects, data-related processes, and concepts. The CCPA introduced a broad definition for personal data (any personally identifiable information)¹²⁹ but including a novelty – relation to the household.

¹¹⁷ For example, in *Class Action (Civil Case) 1634-05-11 Ohad Pinchewski vs. Sony Corporation*, the District court of Tel-Aviv-Jaffa approved an arrangement achieved between the parties following a class action filed against Sony Corporation and other companies, the manufacturers and resellers of the videogame consoles. According to the claimants, sensitive information relating to millions of users worldwide (including Israeli users) was hacked and exposed, due to the security failure of the respondents.

¹¹⁸ In *Class Action (Center) 32672-02-17 Avi Avraham Barak vs. Facebook Inc.*, a pending case, the claimants alleged that Facebook allowed the publication of individuals' pictures without obtaining their consent and created a database containing such pictures. The claimant requested the court to provide an order including provisions that would prohibit such publications and require the deletion of such database by Facebook. Judgement is yet to be rendered by the Court on this matter.

¹¹⁹ Pub. L. 104–191; and see <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>.

¹²⁰ 15 U.S.C. 6501–6505.

¹²¹ 15 U.S.C. § 6801 et seq.

¹²² 18 U.S.C. § 2721 et seq.

¹²³ See <https://www.natlawreview.com/article/california-consumer-privacy-act-effective-january-1-update>.

¹²⁴ For example, as a result: (1) several companies (especially in the tech sector) decided to boost their privacy practices according to CCPA standards; (2) several other states (e.g., New York, Nevada, and Washington) enacted or are considering proposals to amend their privacy laws; and (3) several privacy bills at the federal level have been introduced (although none has passed).

¹²⁵ Cal. Civ. Code § 1798.83

¹²⁶ Cal. Pen. Code § 1546 et seq.

¹²⁷ Cal. Bus. and Prof. Code § 22575 et seq.

¹²⁸ See https://www.engage.hoganlovells.com/knowledgeservices/news/the-challenge-ahead-a-comparison-of-10-key-aspects-of-the-gdpr-and-the-ccpa_1.

¹²⁹ The CCPA defines "personal information" as: "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(o)(1).

The CCPA also defines the term "sale" very broadly. Under the CCPA, "sell", "selling", "sale", or "sold", means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration". Though this definition comprises a wide variety of activities, disclosures to "service providers" are excluded from the definition of a sale.

Some definitions and concepts are similar to other laws. For example, "consumer" is understood to be analogous to the GDPR concept of "data subject"; "business" is analogous to "data controller" and "service provider" is analogous to "data processor". The terms "processing", "pseudonymisation", "third party" and "collection" also have similar meanings as in the GDPR. One of the developments of the CCPA is such definition as to "infer" which means the development of data about the consumer (e.g., preferences, trends, behaviour characteristics, etc.) from the data collected from the consumer or publicly available sources. The inferred data is the data created by the business, which broadens the protection scope of the CCPA.

b) Principles

Central to the CCPA are concepts of consumer (data subject) rights, including rights to access, deletion, and the ability to opt out of the sale of personal information. Additional central principles are accountability, control, and transparency.

c) Subject-matter

The CCPA is more focused on consumer data protection but includes a solid clarification presuming that any law conflicting with the CCPA, but providing a greater level of protection, is supreme to the provisions of the CCPA.¹³⁰ The CCPA from a material legal point of view applies to data collected electronically (e.g., via the internet), but also includes consumer data obtained in a non-electronic way.

d) Territorial scope

The territorial scope of the CCPA is governed by two principles – doing business in California and having residence in California. The consumers' residence criterion is clear but the definition of "doing business in California" is more complicated.

There is a solid definition of a "business":

- annual gross turnover is above USD 25 million;
- such a business buys, receives, or sells the personal information of 50,000 or more Californian residents, households, or devices; and/or
- derives 50 per cent or more of its annual turnover from "selling" California residents' personal information.

The total turnover as a criterium is not very precise as written, because it does not include a qualification of what "turnover" is considered to include: only California, or the entire U.S. or business worldwide. However, in guidelines issued along with its final regulations, the California Attorney General stated that it interpreted this requirement as being total turnover.

e) Data processing subjects' relations

The CCPA introduces a "service provider" concept, whose function is to process the data based on the identified contractual purposes. However, such processing cannot include re-selling or re-transferring of data in a broad sense.

f) Cross-border transfers

The CCPA does not govern the cross-border and out-of-state transfers.

¹³⁰ See Cal. Civ. Code § 1798.145.

g) *Consent*

The CCPA does not articulate in detail the legal bases for data processing. It governs issues of the commercial use of personal data. As a general rule, there is no need to acquire consent for data processing. The consumers are granted the right to "opt-out" of the sale of their data (however, no opportunity to rectify the data) but only in cases when such data is subject to financial incentives (to be sold, for instance). In practice, businesses that sell personal information (as that term is understood in the context of the CCPA) must place a "do not sell my personal data" link on the website which can be used by the data subject. The only strict general limitation in form of an "opt-in" approach is foreseen for minors.

h) *Sanctions, remedies, and enforcement*

The CCPA grants a private right of action (i.e., the ability for consumers to sue a business) only where a consumer's nonencrypted or nonredacted personal information has been subjected to unauthorised access, exfiltration, theft, or disclosure as a result of a business' violation of its duty to implement and maintain reasonable security procedures (i.e., in the event of a breach)¹³¹.

A CCPA violation in form of simple non-compliance with the law can lead to a damage compensation claim within the range of USD 100 up to USD 750, a greater amount considered by a court, or a relief. This approach is connected to U.S. class actions when a number of injured individuals can claim damages caused by the same violator for the same breach. However, to file such a claim, the consumer is required to first notify the business that suffered the data breach and wait for 30 days to give an opportunity to the business to "cure" the data breach. If the business is able to cure the data breach, no compensation claim exists; however, there is little guidance on what is sufficient to "cure" a data breach, and some courts might decide that there is no way to do so if the harm has been done. Most of the CCPA actions have been filed before a federal court, not to the state court, which allows the federal courts to assess the CCPA¹³².

The California State Attorney General (the "CSAG") has the sole authority to enforce violations of the CCPA. The penalty for businesses for actions brought by the Attorney General is limited to USD 2,500 for negligent non-compliance and up to USD 7,500 for intentional violations. Above the penalties, the Attorney General can bring a civil action against the violating companies, which can be multiplied by the number of violations.

3. What is the outcome, and/or impact of the CCPA on business and society?

The CCPA is considered to be a huge, comparable to the GPDR, introduction of data protection legislation for California business. It brings a unified approach and some clarity of how consumer data must be processed. The business can freely process the data on the "opt-out" approach with some limitations. The consumers are provided with simple and clear procedures on how to "opt-out" (but not to correct the data), apply for damages, and protect their rights in a practical manner.

Despite the fact of the recent "coming into force" and limited scope of damage recovery, there are already several class actions on the grounds of the CCPA. Such claims are a huge battleground for CCPA interpretation. They include questions of service provider responsibility¹³³, privacy invasion¹³⁴, sharing the personal data¹³⁵, leakage of the minors and consumers' personal data¹³⁶, and others. Within this year, the CCPA based enforcement can lead to multimillion compensations in class action cases for claimants in the USA.

¹³¹ Cal. Civ. Code § 1798.150

¹³² The first wave of lawsuits filed by individuals shows that many of the defendants are tech companies (e.g., *Hurvitz v. Zoom Video Communications, Inc.* et al., No. 2:20-cv-03400).

¹³³ [Hanna Andersson and Salesforce.com Data Breach Litigation](#) – class action claiming USD 5 million for data breach resulting in a loss of personal data, such as unencrypted credit card information.

¹³⁴ [Sheth v. Ring LLC, Case No. 2:20-cv-01538](#) – class action claiming USD 5 million for privacy invasion caused by the doorbell camera.

¹³⁵ [Zoom Video Communications, Inc. Privacy Litigation \(5:20-cv-02155\)](#) – private action for allegedly illegal sharing personal data with Facebook. (Zoom already removed the relevant sharing stream). There is a number of agreements with plaintiffs leading to dismissal of charges.

¹³⁶ [I.C., a minor, by and through his natural parent, Nasim Chaudhri v. Zynga, Inc. \(4:20-cv-01539\)](#) – class action against an Internet video game owner requiring a relief and damages compensation for the whole class applied for the security breach that lead to a leakage.

For U.S. businesses, the CCPA is about the introduction of the robust data protection compliance according to its standards disregarding the reach of CCPA among other U.S. states. It is considered that the CCPA is the catalyst for other states to implement the same level of data protection within their legal framework.

4. What are the regulatory and oversight bodies under the CCPA?

The CSAG is responsible for the enforcement of the CCPA. By now, some enforcement letters have been sent to business already. These letters essentially state that the CSAG has noticed potential deficiencies with their CCPA practices or disclosures. However, the CSAG is limited to resources. Therefore, the CSAG stated that the "office is likely to conduct only three enforcement actions a year"¹³⁷, which would be quite low compared to, e.g., GDPR enforcement activities.

The CCPA requires the CSAG, as a supervisory authority, to adopt the regulations to the CCPA, which will guide on how to comply with the CCPA and enable consumers to exercise their new rights. On July 2, 2020, the General Attorney submitted the final regulation to the California Office of Administrative Law¹³⁸.

The CCPA establishes a Consumer Privacy Fund within the General Fund in State Treasury, which will be filled up by civil penalties or settlement proceeds and used by the state courts and the Attorney General to fully offset any costs incurred by the state courts in connection with the CCPA.

Data transfer from the EU to the USA – Privacy Shield

The CCPA in comparison to the GDPR does not regulate the aspect of data transfers from the state as well as it does not require the BCR or certification by the supervisory authority. At the same time, the USA is not considered by the EU as a country that ensures an adequate level of data protection. Under the GDPR there was an additional data transfer mechanism foreseen from data transfer from EU to the USA when the recipient belonged to the Safe Harbor and the Privacy Shield repealing the Safe Harbor¹³⁹.

The discussion about the update of Safe Harbor between the EU Commission and U.S. authorities began in January 2014. In June 2014, the Commissioner for Justice provided an update on the negotiations and reported that the Department of Commerce (DOC) had agreed to 12 of the Commission's 13 recommendations. In March 2015, there was a legal claim on the validity of Safe Harbor. The complaint was then escalated to the Irish High Court, which in turn referred the matter to the ECJ. On 6 October 2015, the ECJ issued its judgment and declared the Safe Harbor adequacy decision invalid¹⁴⁰. This ruling increased the pressure on the European Commission to establish a more robust alternative mechanism for transfers of data from the EU to the USA.

On 29 February 2016, the principles of a new EU-U.S. Privacy Shield Framework were established and accompanied by information on how the framework will work in practice¹⁴¹. The Privacy Shield Framework's documentation is significantly more detailed and imposes more specific and exacting measures on organisations wishing to join the framework. In 2016, the EU Commission published a guide to the EU-U.S. Privacy Shield¹⁴².

On 16 July 2020, the ECJ invalidated the Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield^{143,144}. Currently, the data transfers from/to EU is subject to another safeguard application pursuant to Article 46 of the GDPR.

¹³⁷ "California Rings In The New Year With A New Data Privacy Law", December 30, 2019.

¹³⁸ Press Release, 2 July 2020: [Attorney General Becerra Submits Proposed Regulations for Approval Under the California Consumer Privacy Act](#).

¹³⁹ Before the Privacy Shield, the [Safe Harbor scheme](#) was covering EU data transfers: on 26 July 2000, following extensive negotiations, the European Commission issued a decision stating that the Safe Harbor Privacy Principles provided adequate protection for personal data transferred from the EU. Safe Harbor is a mechanism of a self-regulatory framework that allowed transatlantic data transfers for the U.S.-based companies that agreed to abide by the [Safe Harbor Privacy Principles](#). The 7 principles were: notice, choice, onward transfer, data integrity, security, access, enforcement.

¹⁴⁰ [EUCJ Press Release No 117/15](#), Luxembourg, 6 October 2015, Judgment in Case C-362/14, *Maximilian Schrems v Data Protection Commissioner*.

¹⁴¹ [Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield](#).

¹⁴² [Guide to the EU-U.S. Privacy Shield](#) - European Commission - Directorate-General for Justice and Consumers as of 2016.

¹⁴³ A new court proceeding was initiated again by Maximilian Schrems against Facebook at the end of 2015. Mr. Schrems asked the Irish Data Protection Commission to change Facebook's use of Standard Contractual Clauses (the "SCCs"). In this connection, the Irish DPA challenged the whole concept of the Privacy Shield. This was followed by more concerns raised by various [EU data privacy organisations](#).

¹⁴⁴ [Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximilian Schrems](#) (Schrems II).

Section 5. United Kingdom. Data Protection Act of 2018 (the "DPA 2018")

1. What were the pre-requisites for creating the DPA 2018?

In 2018, the UK as an EU member updated its legislation to GDPR standards. On 23 May 2018, the new DPA 2018 came into effect. The DPA 2018 replaced the previous 1998 Data Protection Act¹⁴⁵. Even though the UK left the EU on 31 January 2020 and entered into a transition period of 11 months (the "**Transition Period**"), EU law still applies. Accordingly, until the end of the Transition Period, the GDPR continues to apply in the UK, besides the DPA 2018. At the end of the Transition Period, the UK will become a third country for the purposes of the data transfer provisions within the GDPR and transfers to the UK from the EU will need to be subject to appropriate safeguards (such as SCCs) or an applicable derogation unless the EU Commission adopts an adequacy decision in respect of the UK. Negotiations on this are currently underway between the EU Commission and the UK Government. The Commission issued a statement on 9 July 2020 stating that the EU will do its best to conclude the assessment of the UK regime by the end of 2020 with the view of adopting an adequacy decision rapidly but businesses should be ready to implement appropriate safeguards irrespective of the outcome¹⁴⁶.

2. What are the main provisions of the DPA 2018?

After the end of the Transition Period, the GDPR will become a part of the UK's domestic law under the European Union (Withdrawal) Act 2018¹⁴⁷ and become a UK GDPR¹⁴⁸. Therefore, the GDPR and its principles are and will continue to be UK legislation. The House of Lords also published the Explanatory notes¹⁴⁹ which confirm that the "DPA 2018 and the GDPR apply substantively the same standards to most data processing in the UK to create a clear and coherent data protection regime".

The DPA 2018 regulates the following processing regimes: (1) within the scope of the GDPR; (2) outside the scope of the GDPR; (3) by competent authorities for law enforcement purposes; and (4) by the intelligence services.

The DPA 2018 has seven parts and 20 schedules¹⁵⁰.

- **Part 1. Preliminary:** provides with the general information.
- **Part 2. General Processing:** provides with the aspects of general data processing and also contains provisions extending the GDPR standards. Part two has three chapters.

The term "public authority" is not defined under the GDPR, but section 7(1) of the DPA 2018 includes such definition. Section 7(2) further specifies that a public authority within section 7(1) is only a public authority "when performing a task carried out in the public interest or in the exercise of official authority vested in it". Moreover, part 2 regulates the processing of unstructured manual data held by a public authority. Part 2 also sets out the derogations which provide exemptions from the GDPR. Part 2 of Chapter 2 states that terms used in the DPA 2018 will have the same meaning as in the GDPR subject to any modifications described.

Section 9 of the DPA 2018 sets out that starting from 13 years, a child can consent to process their personal data to provide information society services.

Section 10 of the DPA 2018 implements such derogations allowing the processing of special categories of personal data and criminal conviction data where justification exists.

¹⁴⁵ Its aim was to (1) supplement the GDPR with UK specific provisions and to introduce derogations and exemptions from the GDPR; (2) extend the GDPR to non-EU matters; (3) increase the Information Commissioner's Office's (the "ICO") powers for imposing sanctions and create new criminal offences; (4) set the age from which parental consent is not needed when offering an online service directly to a child (13 years); (5) implement the Data Protection Law Enforcement Directive; (6) provide a specific data protection regime for the intelligence services; and (7) increase the maximum regulatory fines in accordance with the GDPR.

¹⁴⁶ [Getting ready for the end of the transition period with the UK: European Commission adopts "readiness" Communication, 9th July 2020.](#)

¹⁴⁷ [European Union \(Withdrawal\) Act 2018.](#)

¹⁴⁸ According to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 the DPA 2018 requirements will be merged with the GDPR to form a new data protection regime that will work in the UK after Brexit. It is known as the UK GDPR.

¹⁴⁹ [Explanatory Notes relating to the Data Protection Bill](#) [HL] as brought from the House of Lords on 18 January 2018 (Bill 153).

¹⁵⁰ [Data Protection Act 2018](#). Schedules are often used to spell out in more detail on how the provisions of the bill are to work in practice. If a Bill becomes an Act of Parliament, its Schedules become Schedules of that Act - <https://www.parliament.uk/site-information/glossary/schedules/>.

– **Part 3. Law enforcement processing:** defined as "the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". Part 3 establishes rights and obligations for organisations with law enforcement functions and all individuals whose personal data is processed for law enforcement purposes.

– **Part 4. Intelligence services processing:** (1) provides regime, similar to the GDPR, for processing of data by the intelligence services (MI5, SIS (commonly known as MI6) and GCHQ); (2) is based on the standards from the modernised Convention 108; (3) establishes that personal data processing by the intelligence services for national security purposes must comply with all six data protection principles set out in Sections 86-91 of the DPA 2018; (4) establishes rights of the data subjects, data breach requirement, data transfer, and controller and processor obligations all in the connection of the intelligence services.

– **Part 5. The Information Commissioner:** (1) provides for the continuing existence of the ICO; (2) describes powers of the ICO; (3) requires the ICO to prepare, publish and review a number of codes of practice, e.g., data sharing, direct marketing; (4) includes powers to carry out consensual audits; (5) empowers the Secretary of State to make regulations requiring data controllers to pay charges to the ICO (replacing the notification fees).

– **Part 6. Enforcement:** the DPA 2018 created two new offences: (1) knowingly or recklessly re-identifying de-identified personal data without the consent of the controller; and (2) the alteration of personal data to prevent disclosure following a subject access request. It also establishes the responsible director's liability for an offence committed by an organisation. Additionally, it establishes the maximum fines up to EUR 20 million or 4% of the undertaking's total annual worldwide turnover (in accordance with Article 83 of the GDPR). The sum should be converted to pounds.

– **Part 7. Supplementary and final provisions:** contain miscellaneous supplementary provisions and commencement of the DPA 2018's provisions. Most of the provisions came into force on 25 May 2018.

The DPA 2018 also contains a number of other criminal offences, e.g.: (1) intentionally obstructing or failing to assist a person executing a warrant; (2) providing knowingly or recklessly false statements in response to an information notice; (3) knowingly or recklessly obtaining or disclosing personal data without the consent of the controller, or after obtaining personal data, retaining that data without the consent of the controller and others. There are no custodial sentences in respect of offences under DPA 2018 and no powers of arrest; all offences are punishable only by a fine, but some are now recordable offences.

3. What is the outcome, and/or impact of the DPA 2018 on business and society?

UK companies are obliged to comply with both the GDPR and the DPA 2018 during the Transition Period and after based on the UK GDPR.

In October 2018, the ICO issued its first enforcement notice under section 149 of the DPA 2018 on AggregateIQ Services Ltd¹⁵¹ (a Canadian company located outside the EU). In 2019, the ICO issued a notice of its intention to fine Marriott International, Inc. (fine of GBP 99 million)¹⁵² and British Airways (fine of GBP 183 million)¹⁵³ in relation to cyber data breaches. The first fine issued by the ICO was on 20 December 2019 to Doorstep Dispensaree pharmacy. The fine amount was GBP 275,000¹⁵⁴. In addition, the judgment awarded in October 2019 by the English Court of Appeal in *Lloyd v Google LLC* has allowed a representative action to proceed. Although this case was decided under the DPA 1988 rather than the DPA 2018, it could potentially open the way for opt-out class actions for privacy breaches.

¹⁵¹ [Enforcement notice issued to Aggregate IQ Data Services Ltd.](#)

¹⁵² [Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, 9 July 2019.](#)

¹⁵³ [Intention to fine British Airways £183.39m under GDPR for data breach, 8 July 2019.](#)

¹⁵⁴ [Doorstep Dispensaree Ltd monetary penalty notice, 20 December 2019.](#)

The GDPR and DPA 2018 affect UK businesses in a similar way to companies in other parts of the EU. However, it is still challenging for all UK companies to get GDPR compliant. Statistics from 2019 shows that 52% of UK companies are not fully GDPR compliant¹⁵⁵.

The UK GDPR will have the extraterritorial effect (similar to the GDPR) and will also oblige certain organisations caught by the UK GDPR but not established in the UK to appoint a UK representative (again similar to the EU representative concept under the GDPR). Some organisations may need to have representatives in both the EU and the UK after the Transition Period.

In the aspect of processing special categories of data, the provisions of the DPA 2018 are much more detailed than the ones of the GDPR. The ICO has published guidelines on special category data processing¹⁵⁶.

The UK citizens are quite proactive in communicating with the ICO. During the first year of the GDPR enforcement, the ICO has received over 41,000 data protection concerns from UK citizens¹⁵⁷. This is largely due to greater awareness of the law and in particular the enhanced data rights of individuals under GDPR and the DPA 2018.

The ECJ decision may also influence how the UK deals with data transfers from the UK after the end of the Transition Period. For transfers of personal data from the UK to the EEA, the UK government has indicated its intention to ensure that personal data can continue to flow freely from the UK to the EEA and intends to recognise the EEA and jurisdictions subject to an adequacy decision by the European Commission as adequate for the purposes of UK data protection law. It was also anticipated that UK organisations could continue to rely on SCCs or BCRs.

In terms of relying on Privacy Shield, the UK ICO has stated that for the time being, companies currently relying on Privacy Shield to transfer personal data to the U.S. can continue to do so, although organisations not already relying on it should not start to do so now.

In the short term, this statement will be reassuring for UK-based data exporters and suggests there may be a little immediate risk of enforcement action from the ICO for continued reliance on Privacy Shield. However, the ICO has indicated that it is reviewing its current guidance on the SCCs and Privacy Shield in light of the decision so this needs to be kept under review. The longer-term position in relation to the UK to U.S. transfers remains unclear.

4. What are the regulatory and oversight bodies under the DPA 2018?

The ICO has the DPA tasks described in Article 57 of the GDPR, and powers from Article 58 of the GDPR. At the same time, the DPA 2018 clarifies the ICO's obligations and operations. The ICO continues to have many of the existing duties that were set out in DPA 1998, including investigatory, authorisation, and advisory powers (now set out in the GDPR). Moreover, the ICO is very active in publishing guidance and recommendations on the UK's data protection laws. The ICO also has several regulatory powers, similar to the GDPR requirements¹⁵⁸.

Moreover, until the end of the Transition Period, the EDPB and the EDPS continue to be the applicable oversight bodies in the UK.

¹⁵⁵ [PrivSec "#privacy: More than half of UK businesses are not fully GDPR compliant", 12 September 2019.](#)

¹⁵⁶ [ICO's "Special Category Data Guidance".](#)

¹⁵⁷ [ICO: GDPR – One Year On.](#)

¹⁵⁸ The main powers of the UK DPA set out in the DPA 2018 are the following:

- (1) the ICO can charge controllers an annual fee to register that they are processing personal data, unless they are exempt (section 137), there is a three-tier system of fees (£40, £60 or £2900) in the UK¹⁵⁸. ICO also publishes a guide on the fee structure¹⁵⁸. This fee repels the requirement to "notify" (or register), which was in the Data Protection Act 1998.
- (2) Part 6 of the DPA 2018 describes the ICO's civil enforcement powers (e.g., notices, complaints brought by data subjects and the potential remedies that a court can provide).
- (3) The ICO can impose the notices: (1) Information notices; (2) Assessment notices; (3) Enforcement notices; and (4) Penalty notices.
- (4) The ICO has powers entry and inspection (search warrants) and can carry out a dawn raid on non-governmental and non-NHS entities. The ICO has the powers with the consent of a data processor or controller, to conduct a consensual audit to assess whether the controller or processor is complying with good practices in the processing of personal data.
- (5) The ICO has the rights of criminal prosecution, non-criminal enforcement, and audit.
- (6) The ICO is responsible for the development of data sharing and direct marketing codes.

5. How is open data regulated in the UK?

The official regulation of open data in the UK started in 2010 with the creation of Open Government License¹⁵⁹ and the data.gov.uk¹⁶⁰ site by Prime Minister Gordon Brown's administration. The Open Government License is a free and perpetual copyright license for Crown Copyright works, which was published by the UK government. Data.gov.uk is a repository of public sector data, created by the UK Government. Its main aim is to make non-personal UK government data publicly available. Crown copyright is a form of copyright, which applies by default to all government department published documents¹⁶¹.

As of now, there are approximately 30,000 datasets from various departments of the UK government. All data is stored depersonalised and is in a format that allows it to reuse.

The UK's Open Standards Board¹⁶² accepted various open standards for data, e.g., ODT, ODS, CSV, Open Contracting Data Standard and the IATI data standard. In 2017, the Government published new guidance¹⁶³ on what data should be released and how to ensure that it would be easy to find and available in the most usable format.

Critique about the open data in the UK

Since 2013, the UK has been ranked as a leading country regarding open data space¹⁶⁴. Open data has a lot of challenges, including, e.g., uneven data quality and data literacy. Since 2019, the UK open data program's success is declining. The opposite happens in Ukraine, whose open data usage is rapidly developing¹⁶⁵.

In November 2018, the EU Commission has published a report¹⁶⁶, where the UK' reputation as a leading country concerning open data was criticised and started to decline compared to the previous years¹⁶⁷.

Section 6. Turkey

1. What were the pre-requisites for creating the Law on Personal Data Protection No. 6698 (the "TDPL")?

Turkey is a good example for Ukraine as the country applying to the membership to the EU already for more than 50 years. Turkey applied for EU membership in 1987, on the grounds of the Ankara agreement for the co-operation between Turkey and the EEC executed in 1963¹⁶⁸. Since 2016, the EU members' political review of the Turkey integration struggled. Turkey remains a formal candidate for a membership, but in fact, several EU member-states negate the fulfilment of the Ankara agreement and compliance with EU principles from Turkey's side. In terms of data protection, Turkey tries to obtain an EU adequacy decision for free data flows with the EU.

Since 2010, the Turkish Constitution foresees a general right to privacy with a reservation for a legitimate public interest (Article 20(3))¹⁶⁹.

In 2016, the TDPL was enforced¹⁷⁰. The TDPL is mainly based on the Directive with national peculiarities. Data processing issues are also governed by supplementary sectoral and enforcement regulations, e.g., in the field of healthcare, banking and finance, criminal code, etc.

¹⁵⁹ [Open Government License for Public Sector](#).

¹⁶⁰ Website: <https://data.gov.uk/>.

¹⁶¹ [Open Government License for Public Sector](#).

¹⁶² [Open Standards Board Meeting Minutes, 9 December 2019](#).

¹⁶³ [The Prime Minister Personal Minute with Annexes, 14 December 2017](#).

¹⁶⁴ [Global Data Index Rating: UK](#).

¹⁶⁵ [Open Data Barometer Report as of 2018 \(p.8\)](#).

¹⁶⁶ [Open Data Maturity in Europe Report for 2018 \(p.110\)](#).

¹⁶⁷ For example, the UK is not in the list of countries, which "have a predefined approach to ensure the currency of metadata and data. Moreover, licensing of datasets isn't always clearly displayed.

¹⁶⁸ [Agreement Creating An Association Between The Republic of Turkey and the European Economic Community](#) as of 1 September 1963.

¹⁶⁹ [Constitution of Turkey Republic](#) as of 1982 (unofficial translation with valid amendments).

¹⁷⁰ The [Law on Personal Data Protection](#) of Turkey as of 2016.

The TDPL had a two-year grace period for bringing the authorities and society in compliance with the TDPL. The TDPL and related regulations (e.g., regulations governing data controller notification requirement) constituting the data protection regime is completely in force since June 2020.

The TDPL is supplemented by laws regulating the powers of the Turkish Data Protection Authority (the "**KVKK**"): (1) Regulation on the Deletion, Destruction and Anonymisation of Personal Data (28 October 2017) (the "**Erasure Regulation**"), (2) Regulation on Processing and Protecting the Privacy of Personal Health Data (20 October 2016) (the "**Health Data Regulation**"), (3) Regulation on Organisation of Personal Data Protection Authority (26 April 2018) (the "**KVKK Regulation**"), etc.

The KVKK has issued a significant number of guidelines (28) supporting the legislation in various streams by 2019¹⁷¹.

In September 2016 (after TDPL adoption), the EU stated that the Turkish data protection system is not yet in line with EU regulations¹⁷².

2. Main provisions and peculiarities of the TDPL

The TDPL has a lot of similarities with the Directive and has notable differences to the GDPR as it was done before the GDPR was published.

a) Definitions

The TDPL includes all necessary basic definitions for subjects of data processing, personal data, and data processing as the Directive. The TDPL only accepts consent given explicitly.

b) Principles

Article 4 of the TDPL establishes key principles of the data processing: (1) lawfulness and fairness; (2) being accurate and keep up to date where necessary; (3) being processed for specified, explicit and legitimate purposes; (4) being relevant, limited and proportionate to the purposes for which they are processed; (5) being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data is processed.

c) Subject-matter, territorial scope and legal grounds for the processing

The TDPL applies to any data controllers and processors that collect data or process data collected from Turkey, to entities and individuals located within and outside Turkey (automated and non-automated processing).

The TDPL recognises the processing of personal data and processing of sensitive personal data (similar to the Directive). Sensitive personal data can be processed like all other data only on the grounds of explicit consent. The legal bases for personal data processing are similar to the Directive.

The territorial extent of the TDPL allowed the KVKK to impose fines on the foreign data controllers.

d) Cross-border transfers

The TDPL sets a general rule allowing data transfers on the grounds of explicit consent abroad and/or to countries listed by the KVKK having an adequate standard of data protection (no countries listed yet). However, the lawmakers introduced specific amendments to the Banking Law (Article 7) prohibiting financial institutions from transferring personal data home or abroad even when having an explicit

¹⁷¹ [Guideline on Data Protection in Turkey](#) published by KVKK includes reference to the 28 guidelines.

¹⁷² [Answer given by Ms Jourová on behalf of the Commission](#): "As a candidate country, Turkey needs to demonstrate that its data protection laws are in line with the EU acquis (this is also a requirement for visa liberalisation, as well as a prerequisite to conclude an operational cooperation agreement with Europol and strengthen judicial and police cooperation with EU Member States, including on counter-terrorism). The Commission recently indicated that Turkey needs to amend its legislation on personal data protection in order to ensure that it is in line with the EU acquis (notably to guarantee that its data protection authority can act in an independent manner and that the activities of law enforcement agencies fall within the scope of the law)."

consent¹⁷³. The banking authority of Turkey is allowed to specify further if the respective cross-border transfer is allowed and under what conditions.

e) Consent

The TDPL establishes a single concept of explicit consent for all issues with the imposition of the burden of proof on the shoulders of the data controller.

f) Sanctions, remedies, and enforcement

The TDPL foresees administrative, criminal liability and civil actions against the violators:

- the administrative fines range up to appr. EUR 273,000; within 2019-2020, the KVKK represented a number of cases with fines' amounts reaching to the top of this range¹⁷⁴;
- the criminal liability can reach up to four years of imprisonment for a data breach;
- the injured parties can claim damages caused by the violation of the TDPL; there is no opportunity for a class action, however, the legally associated groups of individuals can file a joint claim.

The TDPL does not cover a number of concepts established by the GDPR such as, e.g., pseudonymisation, data portability, DPO appointment (there is only a representative for the registry purpose), privacy by design and privacy by default.

3. Outcome, and/or impact of the TDPL on business and society

The TDPL is the first legal framework for data protection in Turkey. Considering the recent coming into force, it has presented sufficient clarity on how the data should be processed, what are the appropriate legal grounds and the liability for non-compliance. The data subjects were provided with effective protective tools, including civil action. The enforcement extent required foreign data controllers to comply with the TDPL if they process data from data subjects located in Turkey.

However, the TDPL peculiarities seem to be too complicated for having international data flows under the GDPR, mainly due to the following reasons:

- the TDPL is based on the Directive and misses the new regulations adopted by the GDPR;
- the TDPL peculiarities require the foreign controllers to obey its specific requirements above the regular level (e.g., explicit consent for all consent-based processing activities);
- it is not clear yet, how the data subjects civil damage claims will be assessed by Turkish courts and what burden of proof is necessary; and
- class actions are excluded (several forms of infringement can affect a huge number of data subjects).

4. What are the regulatory and oversight bodies under the TDPL?

The supervising DPA under the TDPL is the KVKK. The KVKK structure consists of the Presidency and the Board (the decisionmaker). The KVKK's responsibilities are in line with the Directive requirements. Being a recently established authority, the KVKK has:

- represented a number of administrative penalising cases;
- introduced a BCR application form¹⁷⁵ and a significant number of guidelines;
- established and maintains the Data Controllers' Registry Information System¹⁷⁶;
- required a number of data controllers to rectify the non-compliance in their data processing activities and penalised those who failed to fulfil the requirements; and
- supported the public with broad instructions for legitimate data processing on their website.

¹⁷³ [Banking Law](#) of Turkey with amendments as of 2020 (unofficial translation).

¹⁷⁴ Two separate fines for [Facebook](#) (EUR 242,400 and EUR 250,000), [Marriot International](#) (EUR 220,000), [Dubsplash Inc.](#) (EUR110,600), [Clickbus](#) (EUR 83,300), and [Cathay Pacific Airway Limited](#) (EUR 83,300).

¹⁷⁵ [Binding Corporate Rules application form](#) introduced by the KVKK.

¹⁷⁶ [Data Controllers' Registry Information System \(VERBIS\)](#): information system that is accessible on the Internet and established and managed by the Presidency under supervision of the Board, that data controllers will use for the registration with the Registry and the other operations related to the Registry.

By now, there is no information about successful civil actions based on KVKK enforcement.

5. Pending adequacy decision for Turkey

By now, the EU Commission has not fully assessed the adequacy of protection provided by the TDPL and the effectiveness of its enforcement (there was no official request from Turkey yet).

Considering the pending status of the Turkish data protection regime overview, the introduction of the legal framework and the supervising authority is not enough for awarding the adequacy decision by the EU Commission. Even at the case of total compliance of the legal framework with the GDPR (which is not the case), the EU Commission would seek for:

- the "case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress" (Article 45(2)(a), GDPR); and
- the international commitments of the applicant, in particular in relation to the protection of personal data (Article 45(2)(c), GDPR).

The development of Turkey on the path to an adequacy decision of the EU Commission is a good example for understanding the criteria of an adequate level of protection according to the GDPR. It is notable for Ukraine also because of the additional reasons:

- the TDPL does not govern in detail sufficient concepts of the GDPR (e.g., definitions of specific categories of data)¹⁷⁷;
- the general process of accession to the EU would play a huge role in the perspective of the EU Commission adequacy decision¹⁷⁸.

Part Two – Specific Inquiries

Section 1. Data subject rights, especially, the right to be forgotten. How did governments of analysed countries contribute to the law and procedure on personal data erasure?

Please refer to Annex II for a complete list of data subject's rights in the analysed jurisdictions.

1. The EU and the GDPR

The RTBF is one of the most fundamental and discussed data subject rights that was implemented in the GDPR¹⁷⁹. The need for the RTBF increased over time in a highly technological world, in which any PD can be published in the world wide web with only a limited level of control.

The RTBF was mentioned the first time in Article 17 of the Regulation proposed in January 2012¹⁸⁰. In August 2014, the EU Commission published the Factsheet on the "Right to be forgotten ruling" (C-131/12)¹⁸¹ (the "**Factsheet**"). The Factsheet assesses details on the Case C-131/12¹⁸² (the "**Google Case**"), including the RTBF principle. On 26 November 2014, the 29WP published the guidelines on how the Google Case ruling should be implemented into law and reality¹⁸³ (the "**29WP Google Case**").

¹⁷⁷ The Turkish DPA is using a reference to the GDPR when the TDPL is missing a definition or does not give an understanding of the relevant concepts, such as in the [decisions in 2019 related to the biometric data processing](#), which is, of course, a disclosure of the TDPL weaknesses and a ground for challenging such DPA decisions.

¹⁷⁸ "[Parliament wants to suspend EU accession negotiations with Turkey](#)" as of 13 March 2019. Ukraine would also need to pay attention to the commitments with the EU seriously. Otherwise, it is possible that the political reason can become a "deal-breaker" for the successful adequacy decision.

¹⁷⁹ The GDPR also includes recital 66, which clarifies the need of RTBF, namely "To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data."

¹⁸⁰ [European Commission. Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data](#) (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012.

¹⁸¹ [Right to be forgotten ruling' \(C-131/12\)](#).

¹⁸² Ruling of the CJEU Google Spain SL, Google Inc. v Agencia Española de Protección de Datos [es], Mario Costeja González [Case C-131/12](#) decided on 13 May 2014. According to para 93 of the Case, the data subjects have the right to request data controllers to delete their personal data if the data is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing. At the same time court clarified, that the RTBF is not absolute and will be balanced with other rights, e.g., freedom of expression (para 85). The decision of the Case was that, Google as a search engine is a data controller and is obliged to stop processing and dispatch irrelevant or outdated information in answers to the search results. After the Case decision was published Google received numbers of the deletion requests.

¹⁸³ WP225 [Guidelines](#) on the Implementation of the Court of Justice of the European Union Judgment on "GOOGLE SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ" C-131/12.

The RTBF was included in Article 17 of the GDPR and mainly introduced by recitals 65¹⁸⁴ and 66. On 5 February 2020, the EDPB has published Guidelines 5/2019 on the criteria of the RTBF in internet search engines (Part 1)¹⁸⁵.

Article 17, paragraph 1 of the GDPR sets a list of criteria when the data controller is obliged to delete data without undue delay, e.g., the personal data are no longer necessary to the purposes for which they were collected or otherwise processed¹⁸⁶. Article 17 paragraph 2 of the GDPR foresees the level of obligations of controllers who made the data public (e.g., Facebook). Article 17, paragraph 3 of the GDPR foresees the exceptions based on which a request for erasure can be denied due to the necessity of further processing¹⁸⁷.

2. Germany

Article 58, paragraph 2 of the BDSG grants the RTBF if the following applies: (1) if the processing is unlawful; (2) the processing purpose does not exist anymore; and (3) the data has to be erased to fulfil a legal obligation. Article 58 paragraph 5 and 6 of the BDSG includes notification obligations towards the requesting data subject concerning the RTBF procedure. Article 58 paragraph 3 of the BDSG even foresees the possibility for the controller not to delete the data but to limit its processing if the following applies: (1) indications that the deletion may infringe the protectable interests of an affected natural person; (2) the data has to be stored for proceedings according to Article 35 of the BDSG; and (3) a deletion is impossible or connected to an unbearable effort due to the kind of data storage.

Chapter 2 of the BDSG sets further limitations to data subject's rights (Sections 32-37), including the RTBF for special cases of data processing. According to Article 35 of the BDSG, the data subject's RTBF is excluded in cases of non-automated processing and if the following applies: (1) where erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage; (2) the data subject's interest in erasure can be regarded as minimal; and (3) the personal data have not been unlawfully processed. These more business-friendly restrictions of the RTBF in the BDSG were criticised by the EU during the national law adaptation into the BDSG but included anyway.

3. UK

Part 5 of Schedule 2 of the DPA 2018 contains derogations that processing for the purposes of journalism, academic, artistic and literary purposes constitute "special purposes". Data erasure is not applicable if there is a special purpose for the processing and the controller has a reasonable clarification, that the publication of the material would be in the public interest¹⁸⁸. The controller should evaluate whether there is "the special importance of the public interest in the freedom of expression and information".

¹⁸⁴ According to Recital 65 of the GDPR "A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject."

¹⁸⁵ [Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR \(part 1\)](#).

¹⁸⁶ Article 17(1) of the GDPR The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

¹⁸⁷ (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or (e) for the establishment, exercise or defense of legal claims.

¹⁸⁸ The ICO has issued an explicit Guideline on exemptions applicable to the refusals when the RTBF is requested. Such exemptions include, inter alia, the following:

- Crime, law and public protection;
- Regulation, parliament and the judiciary;
- Journalism, research and archiving;
- Health, social work, education and child abuse;
- Finance, management and negotiations;
- References and exams.

At the same time, Article 47 of the DPA 2018 requires the data controller to delete personal data immediately in some particular cases¹⁸⁹.

Article 53 of the DPA 2018 establishes the concept of manifestly unfounded or excessive requests by the data subject. In the case of deletion based on a request, the data controller may (a) charge a reasonable fee for the request, or (b) refuse to act on the request. The ICO guideline about the RTBF clarifies on how this concept works¹⁹⁰. Its main aim is to protect the business from unreasonable repeatable or overlapping requests from the same data subject.

4. California, USA

According to the CCPA § 1798.105, "A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer." This ruling is quite broad in comparison to the GDPR. At the same time, CCPA § 1798.105(d) allows the business to refuse the requested deletion under 9 derogations¹⁹¹. The CCPA approach is more business-oriented than the GDPR. The USA is a country with a very high standard of freedom of speech with which the RTBF can compete only to a certain level.

In November 2020, the new ballot on privacy will be reviewed in California, namely the California Privacy Rights Act of 2020 (the "CPRA")¹⁹². The CPRA would take effect on 1 January 2021. In contrast to the CCPA, the CPRA is a more GDPR near law and grants the data subjects with more rights, including a more detailed RTBF (§ 1798.105. of the CPRA). The RTBF in the current draft CPRA includes the obligation to delete personal data through all chains of service providers and contractors. The CPRA in its current wording would also establish the following additional rights: expanded opt-out rights, additional requirements for a data breach, expanded definition and special right to limit the use of sensitive personal information, new rights on correction, consent standards and limited retention.

5. Israel

The PPL only regulates the aspect of the RTBF in a reduced way compared to the GDPR. A data subject may only demand, in writing (including in electronic form), from the owner of a database used for direct mailing that the information about him/her be deleted from such a database. The Israeli law further provides the data subjects with the right to rectification of errors (Section 14(a))¹⁹³, namely a person who, on inspecting any information about himself finds that it is not correct, complete, clear or up to date may ask for that data to be amended or deleted.

The Israeli courts are considering cases on the deletion of the information or links, however, not in the context of privacy rights, but more in the aspect of undermining continued defamation¹⁹⁴.

6. Turkey

The application of each of the exemptions should be assessed before application to the RTBF. The relevant Guideline and the examples of the exemptions application is available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/>.

¹⁸⁹ Article 47 of the DPA 2018 Right to erasure or restriction of processing: (1)The controller must erase personal data without undue delay where— (a)the processing of the personal data would infringe section 35, 36(1) to (3), 37, 38(1), 39(1), 40, 41 or 42, or (b)the controller has a legal obligation to erase the data.

¹⁹⁰ [The ICO guideline on Right to erasure](#)

¹⁹¹ CCPA 1798.105(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

- (1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
- (2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.
- (3) Debug to identify and repair errors that impair existing intended functionality.
- (4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
- (5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
- (6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.
- (7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.
- (8) Comply with a legal obligation.
- (9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

¹⁹² [California Privacy Rights Act](#)

¹⁹³ [Protection of Privacy Law, 5741 – 1981.](#)

¹⁹⁴ ["The Right to be Forgotten-the Israeli Version"](#) Computer Law & Security Review, 2018, Tamar Gidron.

Article 7 of the TDPL grants the data subject with the right to be erased, destructed or anonymised¹⁹⁵.

The RTBF was recognised and confirmed by the Turkish Constitutional Court in 2016. It stated that the RTBF applies to both digital and non-digital PD¹⁹⁶. The court also confirmed in general terms a possible balance test based on which the requested erasure can be denied. However, the Turkish law and case-law do not contain specific details comparable to the GDPR.

On 17 July 2020, the Turkish DPA has published a decision¹⁹⁷ on search engines in Turkey. The decision is based on the Google Case decision and 29WP Google Case and includes the following conclusions: (1) the search engine operators are data controllers under TDPA and their activities are data processing; (2) balance test should be done before the data is deleted; (3) the data subjects can go to courts if the data controller does not erase the search results by their request.

Section 2. Processing of special categories of personal data: best practices in analysed countries concerning the processing of biometric and other sensitive data

Sensitive data is considered to be a specific category of personal data that requires additional safeguards according to Article 9 of the GDPR and data protection regimes of other jurisdictions. The compared laws mainly based on the Directive or the GDPR (Turkish TDPL, Israeli PPA, German BDSG and UK DPA) consider at least the following categories of data as sensitive:

- data related to racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health; and
- data concerning an individual's sex life or sexual orientation.

1. The EU and the GDPR

The GDPR concept requires to avoid sensitive data processing. It is allowed to process such data if the goals of data processing (e.g., clinical trials, employment issues) cannot be achieved without such processing. Article 9(2) of the GDPR indicates specific conditions (legal grounds) for sensitive data processing:

- explicit consent of the data subject, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection ("indication by law");
- the vital interests of the person, or of a person physically or legally incapable of giving consent, are at stake;
- by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, processing data about its members or about people in regular contact with the organisation;
- the personal data was manifestly made public by the individual;
- the data is required for the establishment, exercise or defence of legal claims;
- the data is processed for reasons of substantial public interest on the basis of EU or national law;
- the data is processed for the purposes of preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or

¹⁹⁵ [Law on the Protection of Personal Data of Turkey \(unofficial translation\)](#).

¹⁹⁶ The Google Case recognises the RTBF to be only applicable to digital data.

¹⁹⁷ <https://www.kvkk.gov.tr/Icerik/6777/Kisilerin-Ad-ve-Soyadi-ile-Arama-Motorlari-Uzerinden-Yapilan-Aramalarda-Cikan-Sonuclarin-Indeksten-Cikarilmasina-Yonelik-Talepler-Hakinda-Kamuoyu-Duyurusu> (available in only in Turkish).

-
- treatment, or the management of health or social care systems and services on the basis of EU or national law, or on the basis of a contract as a health professional;
 - the data is processed for reasons of public interest in the field of public health on the basis of EU or national law; and/or
 - the data is processed for archiving, scientific or historical research purposes or statistical purposes on the basis of EU or national law.

The GDPR specifically mentions and defines in more detail three categories of sensitive data: genetic data, biometric data, and data concerning health.

Sensitive data processing requires the controller to apply additional procedures and requirements established in the GDPR or required by national law pursuant to Article 9 (4) of the GDPR:

- to introduce a DPO within the data controller structure¹⁹⁸;
- to notify the DPA about the sensitive data processing and register the database¹⁹⁹; and
- to acquire an explicit consent, to conduct a data protection impact assessment, and to introduce specific policies.

The EDPB recently has even issued a guideline related to health data processing in the context of the COVID-19 outbreak²⁰⁰.

In the context of data processing by authorities, the GDPR does not clarify specific requirements. This is due to a far-going approach related to requirements for data processing by authorities, indicated regardless of the data nature (e.g., governmental bodies are also obliged to introduce a DPO²⁰¹). The limited exemptions would be due to data processing in the public interest, such as archiving and scientific purposes (e.g., clinical trials)^{202 203}.

The enforcement of data breach related to sensitive data processing may be not specifically outlined in the peculiarities of sanction evaluation (e.g., there are no separate fines for a sensitive data breach in GDPR). However, specific EU legislation outlines the peculiarity of safeguards provided to sensitive data processing²⁰⁴. Supplementary, the aforementioned GDPR case-law pertaining to the highest fines highlights severe penalties for sensitive data breaches (please refer to Part One, Section 1(3)).

2. Germany, Israel, California, the UK, Turkey

The sensitive data processing is protected by additional requirements imposed on data controllers and processors in each assessed jurisdiction. The minimum requirements would be the data breach notification to the national supervising authority. A number of assessed jurisdictions apply a GDPR approach and required the data controllers and processors to maintain a data register and introduce a DPO (except for the U.S.). None of the assessed law regimes imposes specific requirements for authorities as data controllers or processors (the UK and German approach identifies such subjects separately, but do not impose specific limitations). However, all data controllers and processors are subject to apply additional safeguards. For a comparative overview of Germany, Israel, California, UK and Turkey, please see Annex III. Considering the effective enforcement approach and pro-GDPR concept, Germany and the UK are the most GDPR compliant examples.

¹⁹⁸ Article 37 (b)(3) of the [GDPR](#).

¹⁹⁹ Article 36 (5) of the [GDPR](#).

²⁰⁰ [Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak adopted on 21 April 2020](#).

²⁰¹ Article 37 (a)(3) of the [GDPR](#).

²⁰² [Question and Answers on the interplay between the Clinical trials Regulation \(EU\) 536/20141 and the GDPR](#) issued by European Commission Directorate-General For Health And Food Safety.

²⁰³ [Clinical trials Regulation \(EU\) 536/20141](#).

²⁰⁴ [Law Enforcement Directive \(EU 2016/680\)](#), Article 10.

Section 3. Automated individual decision-making, including profiling: How this issue is regulated in legislation and practice of analysed countries

1. The EU and the GDPR

The GDPR protects the right of the data subject not to be subject to a decision based solely on automated processing, including the profiling, which produces a legal effect or significantly affects such a data subject without a valid legal basis²⁰⁵. In brief, such a right protects the data subject to be subject to a decision on the grounds of data processing by an algorithm, machine, without the involvement of a human being.

The EDPB has endorsed guidelines developed by the 29WP that articulate what is considered to be automated decision making (the "ADM"), profiling and legal, and/or other significant consequences produced by such data processing²⁰⁶.

The legal effect criteria require that the ADM affects legal rights of the data subject (for instance, entitlement to benefit, cancellation of a contract, refused admission to citizenship, etc.). Even in the case of no existing legal effects, it must be considered if another significant impact can exist (e.g., refusal of an online credit application or e-recruiting practices without any human intervention)²⁰⁷. Such a non-legal but significant effect considered to be a wide category of relations that would include inter alia, but not be limited to, the following²⁰⁸:

- decisions that affect someone's financial circumstances, such as their eligibility to credit;
- decisions that affect someone's access to health services;
- decisions that deny someone an employment opportunity or put them at a serious disadvantage; or
- decisions that affect someone's access to education, for example, university admissions.

ADM and profiling are only allowed for private and public controllers if the legal grounds of Article 22 (2) of the GDPR are met, which include the following conditions²⁰⁹:

- for the performance of a contract;
- if authorised by Union or Member State law; or
- with the explicit consent of the data subject.

The contractual obligation and consent as legal grounds are clear and did not require additional clarification. However, the authorisation by the national law was limited to the processing of sensitive data. The GDPR states that decision making based on sensitive data automated processing is only allowed for substantial public interest purposes²¹⁰. The GDPR does not make any difference between the regulatory obligations for the private and public sector as done in other sections of the GDPR. The reasoning behind that is that the outlined legal requirements are on the highest possible level based on which no differentiation seems necessary. The GDPR provides the Member States with the possibility to the extent the requirements for the purpose of data subject rights protection.

2. Germany, Israel, California, the UK, Turkey

The UK²¹¹ has reflected the relevant right within its data protection legislation as a general prohibition for data controllers to apply automated decision-making with a few exceptions. The German BDSG contains an extension of exceptions list allowing automated decision making for health insurance purposes²¹² and the prohibition of the profiling that may be discriminating²¹³. Israel and Turkey reflected the relevant provisions in the way it was formulated in the old Directive, i.e. where the automated decision making was generally

²⁰⁵ Article 22(1) of the [GDPR](#).

²⁰⁶ [Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679](#) adopted on 3 October 2017.

²⁰⁷ Recital (71) of the [GDPR](#).

²⁰⁸ [Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679](#) adopted on 3 October 2017(p.22).

²⁰⁹ Article 22 (2) of the [GDPR](#).

²¹⁰ Article 22 (5) of the [GDPR](#).

²¹¹ Article 96-98 of the [DPA](#).

²¹² Sec. 37 (1) of the [BDSG](#).

²¹³ Sec. 54 (3) of the [BDSG](#).

allowed, but data subjects were provided with the right to object to the processing of their personal data solely by automatic means, which led to unfavourable consequences for the data subjects.

The CCPA, as well as any other federal U.S. law, currently, do not provide protection of the data subjects' right concerning ADM. This issue is governed in the future draft CPRA, which will probably come in force as of 1 January 2023²¹⁴. As of now, there is a report of the EU Commission outlining that the current legal regime of the U.S. does not contain a general prohibition as set out in Article 22 of the GDPR²¹⁵.

The ADM governance remains a huge issue in the EU and across the world in the view of developments in artificial intelligence (the "AI") and facilitation of procedures, especially in the public sector²¹⁶. Despite the fact of a small number of fines imposed for prohibited ADM²¹⁷, the DPAs and the EDPB protect data subjects located in the EU from unallowed ADM mechanisms.

The ADM mechanisms are already established in various e-governance cases around the globe, including, e.g., the following:

- automatic appointment of the court composition for the case (random case allocation);
- profiling of convicted persons; and
- credit profiling.

Considering the discretion granted by Article 22 (2) of the GDPR to the national lawmaker, the EU Member States would need to clarify the proportionate use of the ADM by the public and private controllers. For instance, the French Supreme Court for administrative matters (Conseil d'Etat) stated that "a decision based solely on an algorithmic system could only be legal if the algorithm and its inner workings could be explained entirely to the person affected by the decision. If this is not possible (because of national security concerns, for instance), then algorithmic decision-making cannot be used"²¹⁸. Another case was raised by the Slovenian Ombudsman requiring to re-access a "random facial recognition in airports" by the enforcement authorities as it was obeying data subjects' rights only formally²¹⁹.

The ADM regulations introduced within the GDPR and the laws of the assessed jurisdictions impose high and sophisticated requirements on data controllers and processors regardless of their nature (e.g., public or private). However, considering the abovementioned cases reviewing the approach of the government, the establishment of the ADM and profiling mechanisms should be supported by a robust introduction of the data subject rights. Having a high regulatory standard also seems to be the right choice for avoiding any possible misuse by public authorities and private companies.

Section 4. Certification: do analysed countries conduct certification? Analysis of certification mechanisms, best practices. Qualification and competence of certification body if any?

1. The EU and the GDPR

Before the GDPR came into force, the EU Member States already had certain certifications in data protection (e.g., CNIL seals). At that point, given that the Directive did not have an extraterritorial effect, the

²¹⁴ CPRA shall amend the CCPA text in part of 1798.140. Definitions introducing "profiling". The mechanism of and opt-out form such decision making will be articulated and formalised not later than by 1 July 2022 according to the section 1798.185. (16)(d).

²¹⁵ Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield as of October 2018 (p.40).

²¹⁶ EU sponsors such projects as: (i) DANTE antiterrorism project ("Detecting and analysing terrorist-related online contents and financing activities"); and (ii) iBorderCtrl – "Intelligent Portable Border Control System" – p. 38 of the "Automating Society - Taking Stock of Automated Decision-Making in the EU", a report by AlgorithmWatch in cooperation with Bertelsmann Stiftung, supported by the Open Society Foundations.

²¹⁷ Swedish DPA imposed a fine (EUR 20,000) on a school board for facial recognition data processing without the consent. This case is not precisely a violation of the Article 22 of the GDPR, however, is related to the ADM - <https://www.lexology.com/library/detail.aspx?g=57b07b1c-b9dc-42d3-b30a-1cbe6821139b>.

²¹⁸ P. 69 of the "Automating Society - Taking Stock of Automated Decision-Making in the EU", a report by AlgorithmWatch in cooperation with Bertelsmann Stiftung, supported by the Open Society Foundations.

²¹⁹ The Slovenian Human Rights Ombudsman and the Information Commissioner stated that such a system is not constitutional and filed a formal complaint in 2017. external [SI 18]external [SI 19] The Information Commissioner claimed that the adopted changes of the amended law on the duties and powers of the police external, which gave the police the power to gather the PNR, have legalised some excessive and inadmissible measures for gathering personal data without sufficient protection of citizens that have not been accused or suspected of any wrongdoings, e.g. terrorism or organised crime. They argued that all passengers should not be routinely scanned at the airport just because they are entering the state or landing during the transfer. The Human Rights Ombudsman supported their claims and the Slovenian Constitutional Court will therefore be required to rule on the constitutionality of the latest revision of the law on the duties and powers of the police – p.116 of the "Automating Society - Taking Stock of Automated Decision-Making in the EU", a report by AlgorithmWatch in cooperation with Bertelsmann Stiftung, supported by the Open Society Foundations.

certification mechanisms were aimed at providing a competitive advantage to and confirming the data protection level of its holders.

One of the purposes for introducing a certification mechanism by GDPR was establishing an additional appropriate safeguard for cross-border transfers of personal data outside of EU in the sense of Article 46 GDPR.

Pursuant to Article 46 (2)(f) of the GDPR if a state will introduce appropriate certification mechanism together with the commitments of data processing subjects thereto, transfers to such subjects would be considered as under appropriate safeguards. Such a mechanism requires a state to introduce a robust certification mechanism including articulated rules for achieving a certificate for a three-year period by the controller and processor for certain data processing activities and to allow the data subjects to "quickly assess the level of data protection of relevant products and services"²²⁰.

The GDPR is very specific regarding the requirements for a certification body²²¹ (Art 42 (2) of the GDPR):

- (a) independence and expertise in relation to the subject-matter of the certification;
- (b) respects the criteria referred to in Article 42(5) (can deliver reasons for granting certificates);
- (c) has established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- (d) has established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- (e) demonstrates, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

The certification regulation in the GDPR does not cover all necessary issues and articulate all necessary requirements (e.g., the criteria for the certifying authority is only clearly articulated). The complication of the certification mechanism is elucidated from (i) the legal "infrastructure" requirement to be provided by the relevant state and the EU and criteria for certification; (ii) recognition of the certificates issued by the dispatching and receiving state; (iii) harmonisation of the national certification approach to the EU level; (iv) formal recognition of certification scheme by the EDPB for the non-EU members; (v) challenging requirements for the SMEs; and other issues the national DPAs and certification bodies face when implementing this tool.

Certification can be:

- independent from the national legislation (e.g., ISO/IEC 27018²²²);
- certifications that use the legislation as a source for their substantive criteria, but do not offer compliance with the legislation (e.g., ePrivacyseal EU²²³); and
- certifications that provide assurance of compliance with the legislation (e.g., French DPA seals²²⁴, UK ICO privacy seals).

The GDPR (Article 42 (1)) does not provide with the criteria of compliance that should be met by the certification applicants. Consequently, each Member State, international organisation and a third country would need to develop such criteria on their own²²⁵.

²²⁰ [Recommendations on European Data Protection Certification](#) VERSION 1.0 of November 2017 (p.5).

²²¹ The GDPR does not articulate if the certification body should be a public authority or a private entity. However, considering the certification recognition by the other state, it is recommended to introduce a public entity for certification purpose.

²²² ISO/IEC 27018:2014 "Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors".

²²³ The ePrivacyseal EU claims that it attests a product's "compliance with the list of ePrivacyseal EU criteria, which reflects the requirements imposed by EU data protection legislation." - ²²³ [Recommendations on European Data Protection Certification](#) VERSION 1.0 of November 2017 (p.18).

²²⁴ CNIL provides: "[The privacy seal informs the public that the procedure or product proposed corresponds to the requirements of the Data Protection Authority. In this, it plays the role of a confidence indicator. It does not aim to exempt its holders from administrative formalities.](#)"

²²⁵ By 2017 there was a number of certification legislation acts handling this issue specifically:

- ePrivacyseal EU;

In the case of successful certification establishment, the harmonisation on the EU level remains challenging. The national states already established a number of certification schemes in the data protection field that reflect a specific (national) approach in procedures and certification criteria (e.g., in Germany alone more than 30 certifications in the data protection field already existed by 2017²²⁶).

GDPR (Article 42(5)) allows both the national DPAs and separate certification bodies to perform certification of processing operations conducted by controllers/processors. Where the DPA performs functions of a certification body, it shall distinguish its certification authorities from investigative and enforcement authorities. The accreditation of certification bodies can be performed either by the DPA or national accreditation authorities at the discretion of national law regimes.

German regulators preferred the approach where certification bodies shall receive accreditation to be performed by both the DPA and the national accreditation body. On the contrary, the French DPA (CNIL) performed the certification without reference to GDPR Article 42 itself and intends to continue such practice for the new certification mechanism.

The certification criteria to be yet approved by national DPA and EDPB will cover the following aspects of processing operations: (i) PD; (ii) technical systems – the infrastructure, such as hardware and software, used to process PD; and (iii) processes and procedures related to the processing operation(s)²²⁷.

Yet, there is no best practice of voluntary certification of controllers and/or processors under the GDPR, since EU national DPAs are still in process of developing the certification schemes and certification criteria and their approval by the EDPB.

GDPR satellite countries such as Turkey have only announced the development of the GDPR certification mechanism²²⁸.

Non-EU regional and national certifications mechanism

The U.S. has not yet attributed to the GDPR certification model as many other countries. However, there is a TrustArc APEC CBPR certification applied to cross-border practices of data transfers (the "APEC")²²⁹ and iKeepSafe²³⁰. The APEC is a good example of the data transfer comprehensive certification scheme, however, remains limited to the members of the scheme and participation of privacy enforcement authorities of such members in the APEC Cross-Border Privacy Enforcement Arrangement. Along with that, the members' domestic legislation shall have the effect of protecting personal information consistent with the APEC CBPR system. In this mechanism, countries' local authorities are responsible for the accreditation of accountability agents (analogue of certification body) upon the APEC Joint Oversight Panel (JOP) recommendation. In the U.S., the Federal Trade Commission acts as the privacy enforcement authority, while TrustArc along with three other companies act as accountability agents. There are certain APEC

-
- EuroPrise;
 - CNIL Labels (FR)
 - ICO Privacy Seal (UK);
 - Certification based ON ISO/IEC 27001;
 - Certification based on ISO/IEC 27018;
 - PrivacyMark system;
 - Privacy by Design by Ryerson University and Deloitte Canada;
 - MYOBI, 'Controle krijgen over uw eigen bedrijfsinformatie' (NL); and
 - others.

²²⁶ https://stiftungdatenschutz.org/fileadmin/Redaktion/PDF/Zertifizierungsuebersicht/SDS-Zertifizierungsuebersicht_02_2017.pdf.

²²⁷ Para. 51, [Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation](#).

²²⁸ [November 6, 2019 dated announcement, the Turkish Personal Data Protection Authority announced that it aims to establish a data protection certification mechanism for data controllers and processors.](#)

²²⁹ [TrustArc APEC CBPR certification](#). The Asia Pacific Economic Cooperation, with its 21 Member Countries, including the US, has established a Cross-Border Privacy Rules (CBPR) framework with Accountability Agents certifying data transfer practices. So far, only the US and Japan have accredited Accountability Agents. TrustArc is the Accountability Agent in the US.

²³⁰ [iKeepSafe COPPA Safe Harbor](#) is a topic-specific certification. The scheme aims to ensure that practices surrounding the collection, use, maintenance and disclosure of personal information from children under the age of 13 are consistent with principles and requirements of the US Children's Online Privacy Protection Act (COPPA). It has certified around 10 apps, cloud solutions and web services according to their public register.

CBPR standards (analogue of certification criteria) that the organisations need to comply with in order to obtain the certification²³¹. The certification shall be renewed by companies on an annual basis.

The iKeepSafe was developed to provide the business with the opportunity to ensure the customers that such a business is compliant with the US Children's Online Privacy Protection Act. Apart from iKeepSafe, there are several other Safe Harbor organisations approved by the U.S. Free Trade Commission to certify businesses under the mentioned act.

Currently, being a non-EU certification scheme, the APEC remains a good example for its organisational approach to the oversight bodies²³².

As it was concluded in Data Protection Certification Mechanisms Study on Articles 42 and 43 of the GDPR, the establishment of the certification mechanism as a tool for data transfers remains a challenge even for developed legal regimes (EU countries). There is no single country to be recognised as a "role model" for a certification scheme. However, the recent developments of ICO and UK Accreditation Service (UKAS) in the UK are the most promising in terms of introducing an accredited certifying body, developed rules of certification and complementing the GDPR certification model with non-GDPR schemes.

Section 5. Direct marketing by government institutions and business: What procedures are implied in analysed countries for personal data processing for direct marketing?

1. The EU and the GDPR

The term "direct marketing" is not directly defined in the GDPR. According to recital (47) of the GDPR "The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." At the same time, governmental institutions as a public authority should understand that they cannot rely on the public task basis²³³ while processing data for direct marketing purposes²³⁴. Legitimate interest must not override the interests or fundamental rights and freedoms of the respective data subject. Also, an organisation or public authority may send direct marketing to an individual where the individual has consented to process their personal data for direct marketing purposes. These two different approaches (e.g., legitimate interest and consent) create uncertainty for businesses²³⁵. However, the data controller should choose a single applicable legal basis for data processing²³⁶. At the same time, legitimate interest for the direct marketing is not applicable for the governmental institutions due to the imbalance of public interest weighed against the interests of the data subject. Therefore, the only valid legal basis for publicly owned companies is consent from data subjects. The relevant public owned company or authority can also perform other types of data processing, which can be covered by one or several of the remaining five legal grounds for data processing (e.g., legitimate interest, contractual necessity, public interest, vital interest and legal obligations). Such a public data controller would need to identify unambiguously what exact legal ground would fit for the relevant data processing and apply such a single legal basis. In such a scenario it is also possible to combine consent as a legal basis for several data processing streams. Above the regular requirements for the consent, the consent form would need to distinguish granularly the data processing activities (e.g., streams of data processing) that are consented by the data subject²³⁷.

²³¹ <https://trustarc.com/consumer-info/privacy-certification-standards/>

²³² [Data Protection Certification Mechanisms Study on Articles 42 and 43 of the Regulation \(EU\) 2016/679 \(p.5\).](#)

²³³ Article 6(1) (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

²³⁴ Recital 47: "Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks".

²³⁵ According to new GDPR principles, each processing activity can only be based on one legal basis only, without the possibility to fall back on another option if one option falls out.

²³⁶ Pursuant to para. 123 of EDPB "[Guidelines 05/2020 on consent under Regulation 2016/679](#)" there should be a single legal ground for data processing – "the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilize the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis, which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is."

²³⁷ Recital 32 of the GDPR: Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

The most common and reliable way to obtain consent online is by using an opt-in tick box mechanism. An "opt-in" is where the recipient is asked whether they would like to provide consent by actively ticking a box. It allows the individual to express their wishes in a clear, unambiguous and recordable manner.

According to Recital (70) of the GDPR²³⁸, the data subjects have the right to object from direct marketing. The same is supported in Article 21(3) of the GDPR: "if the person objected from direct marketing, the personal data shall no longer be processed for such purposes". The EDPB has not yet published a guideline on direct marketing.

Direct marketing requirements also apply to children. Direct marketing is forbidden for children under 16, without parental consent. Some Member States in their national laws can decrease the age level to 13²³⁹. Moreover, according to recital 38 "children merit a specific protection when their personal data is used for the purposes of marketing because they may be less aware of the risks, consequences and safeguards concerned"²⁴⁰.

Applicable laws to direct marketing are the GDPR and the Privacy and Electronic Communications Directive (2002/58/EC)²⁴¹ with amendments based on the Directive 2009/136/EC²⁴² (the "**ePrivacy Directive**"). The ePrivacy Directive foresees the obligatory consent for unsolicited electronic direct marketing communications (Article 13), which includes live telephone calls, automated calls, faxes, text messages, video messages and emails.

On 10 January 2017, the EU Commission adopted a proposal for a Regulation on Privacy and Electronic Communications²⁴³, which should have entered into force alongside the GDPR. However, as of now, its implementation remains subject to ongoing negotiations.

2. Germany

In November 2019, the German DPA has published guidance²⁴⁴ on the processing of personal data for direct marketing in accordance with the GDPR. The guidance clarifies the following: (1) more broad understanding of the term "marketing" which in addition includes customer satisfaction surveys and emails for Christmas or birthday parties; (2) concept of balancing of interest; (3) direct marketing is possible if it is fair, proportionate in relation to the marketing purpose, and transparent; and (4) the compatibility test for data controllers. The mentioned guidance includes a lot of examples of marketing approaches and confirms the applicable GDPR and BDSG requirements, which are mainly explicit consent and the weighing of interests of the controller and the DS.

The German antitrust legislation for marketing, namely the German Act Against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb) as last amended on 18 April 2019 (the "**AUC**")²⁴⁵, also includes regulations about direct marketing.

The AUC stipulates that direct marketing activities require the prior explicit consent of the recipient (principle of opt-in). The consent is required for all types of marketing, including by email, SMS, unsolicited

²³⁸ Recital 70: "Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information".

²³⁹ Article 8 (1) of the GDPR "Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."

²⁴⁰ Recital 38: "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."

²⁴¹ [Directive 2002/58/EC](#) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

²⁴² [Directive 2009/136/EC](#) of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

²⁴³ [Announcement of a Proposal for a Regulation on Privacy and Electronic Communications.](#)

²⁴⁴ [Guidance for processing personal data for direct marketing purposes under the GDPR.](#)

²⁴⁵ [German Act against Unfair Competition.](#)

communications to individuals and companies. German courts stressed that there is a need to obtain an explicit consent for the direct marketing purposes as well as to use a double opt-in²⁴⁶. The AUC provides with exceptions where explicit opt-in is not required (section 7(3) of AUC)²⁴⁷. The consent can be revoked at any time as well as the data subject has the right to object and other rights foreseen by the GDPR. The AUC further prohibits direct marketing e-mails if (1) the identity of the sender is disguised or concealed; or (2) if an opt-out address is not provided at all. Consent is the only legal basis for direct marketing in Germany for both public authorities and private companies.

Direct marketing for children foresees similar regulations in Germany as under the GDPR.

The AUC foresees enforcement actions and fines for non-compliance with its provisions: (1) any kind of unsolicited marketing communications may result in warning notices and cease-and-desist actions against the communicator by their competitors, consumer protection bodies or other comparable associations, the Chamber of Trade and Industry and the Chamber of Crafts (*Section 8 of AUC*); (2) if the consumers receive a telephone or automatic calling machine call for marketing purposes without having given consent, fines up to EUR 300,000 may be imposed (*Sections 20 (1)-(2) of AUC*); (3) an entity that has made unauthorised marketing communications can receive damage claims from its competitors (*Section 9 of AUC*).

3. The United Kingdom

In the UK, direct marketing is defined in Section 122(5) of the DPA 2018 as: "the communication (by whatever means) of advertising or marketing material, which is directed to particular individuals"²⁴⁸.

The Privacy and Electronic Communications (EC Directive) Regulations 2003²⁴⁹ ²⁵⁰ (the "**PECR**") accompany the DPA 2018 and clarify the aspects of direct marketing. The PECR is based on the ePrivacy Directive. The PECR covers marketing by phone, fax, email, text or any other type of electronic mail and prohibits unsolicited marketing by the same means of communication. The ICO has clarified that: "The relationship between PECR and the GDPR is slightly different to that between PECR and the 1998 Act, but this does not affect the marketing rules and organisations must continue to comply with both regimes."²⁵¹ The PECR prohibits direct marketing if: (1) the identity of the sender is disguised or concealed; or (2) if an opt-out address is not provided. Moreover, consent is the legal basis that can be used for direct marketing. The business can also rely on one of the derogations²⁵² known as soft opt-in. If the company is using soft opt-in it must provide in each communication an opportunity to opt-out (unsubscribe) (Section 22(3) of PERC). The PECR prohibits sending "unsolicited communications for the purposes of direct marketing" without the prior consent of the data subject. The identity and address of the sender must be included in each communication (Section 23A PERC).

Similarly, to the GDPR, the DPA 2018 foresees for the public authorities to rely either on consent or legitimate interest as a legal basis for direct marketing. At the same time, authorities cannot rely on the basis of public task interest for direct marketing, as direct marketing does not fall under any official duty of the public authority. Therefore, in practice, public authorities will have to rely solely on explicit consent as a legal basis for processing.

In the UK direct marketing for children is both regulated by the GDPR requirements (described above) and

²⁴⁶ [TaylorWessing Global Data Hub " Direct marketing – the German approach"](#).

²⁴⁷ This exception applies if all of the following conditions are satisfied: (1) The entrepreneur has obtained from the customer the latter's electronic mail address in connection with the sale of goods or services; (2) The entrepreneur uses the address for direct advertising of its own similar goods or services; (3)The customer has not objected to this use; and (4) The customer has been clearly and unequivocally advised, when the address is collected and each time it is used, that they can object to such use at any time, without costs arising by virtue thereof, other than transmission costs pursuant to the basic rates.

²⁴⁸ Article 122(5) of the [UK DPA 2018](#).

²⁴⁹ [Privacy and Electronic Communications \(EC Directive\) Regulations 2003](#).

²⁵⁰ [Guidance on PECR](#).

²⁵¹ [ICO guidance on Direct Marketing, page 8](#).

²⁵² Article 22 (3) of the PERC: A person may send or instigate the sending of electronic mail for the purposes of direct marketing where—

(a)that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

(b)the direct marketing is in respect of that person's similar products and services only; and

(c)the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

by PERC, where a parental or guardian consent is a valid legal basis for direct marketing to children, who are under 13.

The ICO is probably one of the most active in the publishing guidelines on direct marketing, which include several guidelines²⁵³.

Except to the fines foreseen for non-compliance with the DPA 2018, the ICO can impose fines of up to GBP500,000 for failing to comply with the PECR. For the period of 2018-2019, the ICO has received approximately 140,000 complaints about electronic direct marketing. In March 2020, a CRDNN Limited was penalised by ICO with a fine GBP500,000 for making more than 193 million automated nuisance calls²⁵⁴. CRDNN Limited became a subject of interest when ICO received more than 3,000 complaints from the data subjects on nuisance calls.

4. California, USA

The CCPA does not have the definition or the concept of direct marketing, however, requires to comply with the CCPA rules. Marketing activities are listed in the CCPA as a type of legitimate business use of personal information. The CCPA requires to provide the data subject with the information about (1) what information is collected, and (2) how the consumers' personal data will be used, e.g., whether the personal data will be shared with any third party and the categories of third parties with whom data will be shared, including marketing providers. Under the CCPA data subjects do not have the right to object but they can request their data to be deleted.

CCPA remains silent on the legal basis for direct marketing as well as on how direct marketing should be done by governmental institutions. However, the current CPRA draft governs the question of marketing, and already suggests the definition of advertisement and marketing²⁵⁵, cross-context behavioural advertising, and establishes the concept of non-personalised advertising²⁵⁶. Under CPRA, Californians will be granted with the right to prohibit the use of sensitive personal data for advertising or marketing.

The Children's Online Privacy Protection Act of 1998²⁵⁷ (COPPA) is a U.S. federal law that governs the privacy of children under 13 years. COPPA includes restrictions on the types and methods of marketing for those who are under 13. Parental consent is required for all actions related to the data of children under 13.

5. Israel

Part 2 Chapter 2 of the PPL governs the direct marketing issues. According to the PPL, "direct mailing" means contacting a person directly based on his belonging to a group of the population that is determined by one or more characteristics of persons whose names are included in a database. "Direct mail services" are defined as "the provision of direct mail services to others by way of transferring lists, adhesive labels or data by any means whatsoever". There is a set of requirements for the direct emails and each must include the following: (1) that it is a direct mailing; (2) the registration number of the databased used for the direct mailing; (3) name and address of the owner of the database; (4) sources from which the owner of the database received this information and (5) that the recipient of the has the right to be deleted from the database and the address to be contacted for this purpose.

According to the PPL, a controller is obliged to register a database with the Database Registrar, a department of DPA, if the database, along with other data, contains data used for direct marketing services.

In June 2017, the Israel DPA has issued guidance on direct marketing and direct marketing services²⁵⁸.

²⁵³ [Guide to Privacy and Electronic Communications Regulations, The rules around business to business marketing, the GDPR and PECR, Direct Marketing guide, Direct marketing code of practice, Direct marketing checklist.](#)

²⁵⁴ Court decision <https://ico.org.uk/media/action-weve-taken/mpns/2617282/crdnn-mpn-20200226.pdf>

²⁵⁵ "Advertising and marketing" is "a communication by a business or a person acting on the business's behalf in any medium intended to induce a consumer to obtain goods, services, or employment." CPRA § 1798.140(a)

²⁵⁶ "Non-personalized advertising" meaning "advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business, with the exception of the consumer's precise geolocation." CPRA § 1798.140(t).

²⁵⁷ [Title 15 - Commerce And Trade, Chapter 91 - Children's Online Privacy Protection.](#)

²⁵⁸ [Direct Mailing guidance of 21 June 2017.](#)

The PPL does not regulate the question of direct marketing to children. However, The Consumer Protection Regulations (Advertisement and Marketing Directed at Minors) 1991 foresees that the advertising and marketing of minors can be done only with the parental or guardian consent.

Supplementary to the PPL, the Communications Law²⁵⁹ (the "**Spam Law**") requires opt-in for distribution of promotional material by email, facsimile, automated dialling systems and SMS (Section 30A(b)). The Spam Law requires that all electronic promotional messages include a clear notice with the information about notification of the recipient's right to opt-out of receiving promotional messages and means for opting-out (including an email address for email advertisements). Consent may be obtained in writing, by electronic message or recorded conversation. Consent is a valid legal basis that can be used by business and governmental institutions to sell direct marketing.

Data subjects have the following rights: (1) to object to (to opt-out) of direct marketing; (2) to require the deletion of their personal data from a database used for direct marketing; (3) the data not to be transferred from a database used for direct marketing services. The data subjects request should be answered within 30 days. Misuse of a database for the direct marketing purpose can result in the administrative fine, e.g., managing or possessing a database used for direct mail services without designation of such use in the database registration.

6. Turkey

The TDPL does not govern specifically direct marketing. Generally, the TDPL prohibits personal data processing without the explicit consent of the data subject (Article 5(1)). Specifically, the Regulation on Commercial Communication and Electronic Commercial Messages No. 6563 (the "**E-Regulation**")²⁶⁰ prohibits sending electronic messages without the prior consent of the recipient, however, such consent is not required in B2B relations, unless the recipients do not opt-out. The consent should be in writing or provided via any channel of electronic communication. The E-Regulation provides with the exemptions when electronic messages can be sent without the recipient's approval²⁶¹. The E-Regulation defines electronic commercial communications as messages with commercial purposes sent via telephone calls, call-centres, fax, auto-diallers, smart voice recorders, email or SMS.

The TDPL and E-Regulation do not govern the children data processing, including direct marketing to children.

On 4 January 2020, the E-Regulation was amended²⁶² by introduction of the following novelties: (1) if the data subject refuses to receive commercial electronic communications, the sender must stop sending the messages within three days; (2) the establishment of the centralised opt-in and opt-out register. Companies, willing to send commercial messages, should have registered by June 2020 and upload previously received opt-in.

On November 2018, the Turkish DPA published a decision 2018/119 on direct marketing, stressing out the consent basis as the only valid ground for direct marketing²⁶³.

IV. FINAL CONCLUSIONS AND RECOMMENDATIONS

The future update of the UkrDPL should take into account (1) current regulatory requirements necessary to cope with the level of mass processing of personal data (especially within the field of social media); (2) a fast-changing data processing environment on an international level; (3) the necessary higher level of protection of children and minors concerning their personal data; (4) the update of industry data protection standards for a useful "selling point" for Ukrainian based businesses (for outbound business and attracting investments from outside) to stay competitive on a global market; and (5) the obligations of Ukraine towards

²⁵⁹ [Communications Law of Israel](#).

²⁶⁰ [Regulation on Commercial Communication No. 6563](#) (available only in Turkish).

²⁶¹ Electronic message to be sent without the approval of the recipient where the message: (1) relates to the change, use or maintenance of goods and services, and the recipient has given its details for that purpose; (2) relates to a continuing subscription, debt collection, updates or the notification of a purchase or delivery; (3) is sent due to a legal requirement; and (4) is an information update sent by brokerage companies in capital markets to the customers.

²⁶² [Regulation amending the Regulation on Commercial Communication and Electronic Commercial Messages](#) dated 4 January 2020 (available in Turkish).

²⁶³ [Article on Turkish DPA decision 2018/119](#).

other countries and international organisations based on international law (e.g., EU Ukraine Association Agreement).

Under the comparison of the above-mentioned data protection law regimes, the question arises what wording and concepts of other countries Ukraine should adopt in the new UkrDPL. The GDPR provides the highest standard of data protection compared to all other non-EU countries compared above. However, the GDPR is also causing most of the challenges, including additional organisational streams and higher costs for businesses which need to comply with it compared to other non-EU data privacy laws.

1. Conclusions for the new UkrDPL

a) The importance of the GDPR

The on-going implementation of European standards and the process of rapprochement towards full membership in the EU request an updated Ukrainian data privacy regulation on European standards. The Ukrainian data privacy environment changed very strongly since the latest enforcement of the UkrDPL, which was mainly based on the Directive. Due to the immense increase of data processing activities online, also in Ukraine, especially in the field of big data and social media, Ukrainian law needs a full update of practical regulations and its enforcement. Ukraine is becoming more and more attractive for back offices or nearshoring centres of companies headquartered in Europe or the Americas (mainly Canada and the US). Ukrainian business mostly affected by data privacy regulations (e.g., the Ukrainian IT and telecommunication industry) have their core client base in Europe²⁶⁴. The Ukrainian business is not only updating its privacy streams and internal organisations concerning personal data processing based on the expected update of the Ukrainian Data Privacy Law to EU standards^{265 266}. Ukrainian businesses are being forced by their European customers and their expectations to already comply with GDPR standards. The majority of those Ukrainian-based businesses having personal data processing as a core requirement for running their business need to uplift their internal standards to comply with the GDPR solely for competitive reasons. Ukrainian business which offer services and goods to EU residence or which monitor the behaviour of data subjects located in the EU, also automatically fall into the scope of the GDPR according to its Article 3(2). The GDPR itself foresees the possibility of DPAs of EU Member States to enforce the GDPR on the soil of Ukraine. This will also happen and is not only a theoretical risk. We expect that now, after two years of enforcement of the GDPR EU internally, the European DPAs will also start enforcing the GDPR against controllers and processors, which processing is located outside of the EU and fall into the extraterritorial scope of the GDPR.

Even US-driven businesses increasingly comply with European standards to stay competitive on the international market. The latest ECJ court decision regarding the US Privacy Shield further supports the necessity to be compliant with the GDPR from the outset and not to rely on Privacy Shields. Also, the Californian CCPA and the future CPRA foresee several regulations similar to the GDPR.

b) GDPR principles and concepts that we suggest not to include in UkrDPL

We suggest not to include the full wording of the GDPR as a "copy-paste" version into the new UkrDPL. We suggest not to copy or to adjust, especially, but not exclusively, the following GDPR principles and concepts:

- Extraterritorial scope (please see above, under I., Section 1., 2.1. b)): we would not include the extraterritorial scope of the GDPR to UkrDPL. This would make processing activities with Ukrainian data subjects much harder for foreign companies and, therefore, reduce the competitiveness of Ukrainian businesses on a European and global level. It is also not expected that foreign businesses and countries will adjust their law and internal organisational streams based on Ukrainian law. It is more probable that Ukraine will be less attractive for outside businesses and choose other countries to work with.

²⁶⁴ OEC statistics about Ukrainian exports: <https://oec.world/en/profile/country/ukr/>.

²⁶⁵ Report On Implementation Of The Association Agreement Between Ukraine And The European Union In 2017.

²⁶⁶ Chapter III of the EU UKR Association Agreement.

-
- EU-like supervisory institutions: we suggest not to establish in Ukraine similar institutions like the EDPB and the EDPS. The concept of a European DPA is outlined above (under I., Section 1., 4.).
 - Similar cross-border transfer requirements: the updated and much more detailed possibilities to safeguard a cross-border transfer from the EU to outside seems in many ways not necessary and also nor realistic to implement in Ukraine. From the options outlined in the GDPR part (above, under I., Section 1., 2.5.), we suggest copying the mentioned (1) EEA jurisdictions; (2) jurisdictions with an adequacy decision from the EU Commission; and (3) specific legal bases into Ukrainian law. SCCs, BCRs, certifications according to Ukrainian law are not necessary. It is practically hard to establish the necessary administrative streams within Ukraine and from the concept not applicable to one country only. We further suggest excluding from the current UkrDPL the option to transfer data to countries that have signed the EU Convention for automated processing due to the fact that many of the signees are not assessed to have a safe data protection regime under European standards. We further suggest keeping the option of an adequacy decision from the Ukrainian authorities but suggest providing this decision with the new Ukrainian DPA and not with the government. The fact that there is not one decision by the government since the enforcement of the current law shows that the current applicability of the government is not practical at all.
 - Similar penalty fines: the concepts of GDPR penalty fines is quite complicated and very strict. The Ukrainian reality would need much stronger enforcement of data protection law and much stricter case law and administrative penalisation conducted by a much more powerful DPA. However, the concept outlined in Article 77-84 of the GDPR, especially in Article 83, would not be practical for the Ukrainian reality. All non-EU countries uplifted the level of penalties significantly. Also, this is recommendable for Ukraine. However, we suggest limiting the administrative penalties to a maximum of EUR 50,000 (like, e.g., Germany) for each violation (not EUR 20,000,000 or 4% worldwide turnover like the GDPR).
 - EU specific regulations: we suggest not to include all regulations from the GDPR, which are purely based on EU specific realities into the new UkrDPL. These include, e.g., the Articles 60-76; 92-93; 94-99 and parts of Articles 51-59 and 85-91.

c) GDPR principles and concepts that we suggest including in UkrDPL

All other concepts and principles also reflected above (please see above, under Part One, Section 1., 2.) can be implemented in UkrDPL. This includes, e.g., subject-matter, objectives, material scope; definitions; main principles of data processing; data subject rights; updated roles and obligations of controllers and processors; cross-border transfer (partly); and independent supervising authority (without the specifics like EDPB role and leading DPA role).

The most crucial factor will be the establishment of an independent and powerful new Ukrainian DPA, which will have all rights and obligations European DPAs have. One of the main roles the new Ukrainian DPA must take over is the education of Ukrainian business and society concerning data protection principles and regulations²⁶⁷. The new DPA must, e.g., pro-actively publish guidelines, attend administrative court proceedings against wrongdoers and must initiate violation procedures on a daily basis. For this, a certain budget needs to be provided and resources are necessary way beyond the current resources provided to the current DPA.

d) Potential impact for Ukrainian businesses and society

An update to GDPR standards would be challenging for Ukrainian businesses in the same way as it is burdensome for European businesses (please see above, under I., Section 1., 3.). The main challenges may include, e.g., (1) non-existing practical support from the national DPA; (2) lack of educated employees; (3) difficult technical adaption; (4) lack of financial resources; and (5) lack of support within the company. As

²⁶⁷ However, this does not mean that most businesses need to be GDPR compliant. As outlined for the UK, in 2019, more than 52% were not GDPR compliant. However, the UK is expected to obtain an adequacy decision before exiting the EU completely.

in Europe, it is expected that the midsize companies will have the biggest challenges to update their internal processes to comply with a GDPR compliant UkrDPL.

However, due to the fact that the high-level business relationship with European customers practically already forces Ukrainian businesses to get compliant with the GDPR and other EU regulations, they started to implement already to keep or get more competitive advantages on a European level. Those Ukrainian businesses, which did not start to implement would be forced by a new regulation to uplift their standards of data protection to European levels. Therefore, they would be able to enter the European market on a more competitive level with their competitors located in Europe. This would possibly open new possibilities for Ukrainian businesses to obtain a higher portion of outbound business with Europe.

In case of an update to GDPR standards and much stronger enforcement, paired with a high level of education and accompaniment by the new Ukrainian DPA, the Ukrainian society's impact would be an improvement in many ways. Minors would be protected on a higher level from any damages connected to data processing. Specific Ukrainian industry sectors would need to protect PD of Ukrainian data subjects more, and the awareness of the importance of PD and its value on a private and business level would increase. Ukraine would make a big step towards a higher level of confidence concerning its overall compliance approach and reputation on a global level. From a protection level, it would be similar to European countries, under the requirement of an independent and powerful new Ukrainian DPA and stricter enforcement of DP regulations by the UkrDPA, the prosecutor department and Ukrainian courts.

e) Potential EU adequacy decision for Ukraine

If Ukraine would like to apply for an EU adequacy decision (for further details, please see above, Section 1., 5., a)), an updated UkrDPL mainly based on GDPR principles would be necessary.

Ukraine would, beside an updated law, also need to have in place strong enforcement of data privacy regulations on the European level, including a visible data protection case-law and an independent and powerful new Ukrainian DPA. According to our assessment, both of them seem not to be on an adequate European level yet to fulfil the requirements for an adequacy decision.

Especially, the example of Turkey shows that an adequacy decision is not only depending on formal fulfilments (like an updated law and a DPA publishing 28 guidelines in a short period of time), but also on the level of practical enforceability of data subject's rights. The EU Commission especially assesses the independence of the national DPA and the activities of all law enforcement agencies, which enforce data protection regulations. This would also include the Ukrainian prosecutor department for criminal misconduct and case law before criminal, administrative and civil courts.

Ukraine would also not be comparable with the UK, which leaves the EU after being compliant with all its regulations. So, an adequacy decision for the UK will be much easier to obtain than for Ukraine.

Israel's adequacy decision shows that a data protection system may also be established on a different legal general regime than the GDPR. However, also the Israeli law needed to adjust to European standards before receiving the adequacy decision in 2011, mainly based on passing the requirements of the WP12. Israel also already had a good law enforcement and case law of Israeli courts confirming principles which were not introduced in the national law at that time, but which are essential to comply with then EU law. The current assessment would also be much stricter and harder to fulfil than the requirements solely based on the WP12, that was published nine years ago.

One positive argument can be that Ukrainian courts already need to include case law of the ECHR into their decision (based on Article 17 of the Law of Ukraine "On the Fulfilment of Decisions and Application of Practice of the European Court of Human Rights" as of 23 February 2006). However, concerning data protection, Ukraine also needs to prove the existence of EU principles confirmed and developed by Ukrainian courts although not yet implemented in Ukrainian law.

Overall, the receipt of a positive adequacy decision seems to be challenging but not impossible. From a political point of view, the EU Commission may grant Ukraine an adequacy decision nevertheless, however,

with certain restrictions. We also expect the process towards an adequacy decision to be unfolded within 2 years after applying for the same and to amend several prerequisites from a judicial, executive and legislative perspective in Ukraine. Therefore, our suggestion for Ukraine would be to apply for an adequacy decision and establishing an on-going consultation with the EU Commission about the necessary changes Ukraine needs to implement to fulfil certain categories.

f) Privacy Shield for Ukraine

The recent ECJ decision about the U.S. Privacy Shield underlines the risks connected to this approach. The UK Privacy Shield would also be based on different regulatory prerequisites than US law. The UK data protection law already complies with the GDPR and will continue doing that also after the legal Brexit for a longer period of time. Overall, we suggest not to apply for a privacy shield for Ukraine to exclude possible legal uncertainties for the future and to have a more robust approach for EU compliance in the long term.

g) Recommendations for the new UkrDPA

We suggest implementing the UkrDPA organisational structure compliant to the requirements of the GDPR (please see Part One Section 1., 4.) and with the consideration of the continental GDPR jurisdiction (e.g., Germany). Although Germany is a federation, the German DPA is a robust executive authority that is a good example for a unitary state as well (e.g., the federal DPA would be an example of a national DPA). It is recommended to implement a separate independent UkrDPA that would not be directed by any executive authority, including the sponsoring ministry. UkrDPA should be headed by the data protection commissioner (the "DPC") that would be offered for election by the Cabinet of Ministers of Ukraine, elected by the parliament and appointed by the President for the term of 4-5 years. The recommended requirements for the DPC would need to include at least the 5-year experience in the data protection field and compliance with the public officer requirements.

It is furtherly recommended to adopt an internal organisational structure of the UkrDPA that would include the deputy DPCs and departments headed by the deputy DPCs that would support the fulfilment of the DPC duties in the following fields:

- investigation of data breaches, data subject claims and auditing the data controllers and processors;
- fine imposition and claim application (e.g., including the judicial redress support);
- development of the data protection legislation (e.g., including compliance with the GDPR) and the UkrDPL guidelines;
- data protection during investigation procedures and intelligence duties performance;
- international data protection relations (e.g., cross-border data transfers, SCCs, certification);
- internal data protection relations (e.g., labour, consumer, IT); and
- UkrDPA secretariat (e.g., HR-department, compliance department, audit department, budget/procurement department, etc.).

The UkrDPA should be entitled to hire the employees at its own discretion. We also recommend supporting the UkrDPA with the legal opportunity to benefit from the fines imposed for the data protection regime violations. We further suggest to include severe reporting obligation of the DPC before the Parliament in respect of (i) the planned and performed enforcement actions; (ii) legislative developments; (iii) level of business and society awareness and commitment to data protection rules; and (iv) anti-corruption compliance commitments.

The offered organisational requirements inspired by the German DPA model are considered to be the best option within the DPA models of the assessed jurisdictions due to the following:

- the UK ICO is a GDPR-compliant DPA model, however, is less applicable for the continental jurisdiction;
- the Californian model would barely fit with the GDPR adequacy criteria in part of the requirements to the DPA; and
- the Israeli and Turkish DPA are mostly based on the aged Directive approach and would not reflect the updated adequacy criteria in part of the DPA enforcement (e.g., the Israeli PPA was accused to be reluctant to investigate data breaches committed by the public data controllers).

2. RTBF and other data subject rights for the new UkrDPL

We suggest updating the list of data subject rights according to the wording of the GDPR (please see Part Two, Section 2., 1.). We also suggest the new Ukrainian DPA to guide the Ukrainian society similar to the

guidelines published by the member-states DPAs, 29WP and the EDPB (e.g., 29WP Google Case). As a possible broader approach and a limitation of the RTBF, the German model can apply. However, it is expected that the EU Commission will not accept such an RTBF limiting approach as outlined in the German BDSG when deciding about an adequacy decision. The German lawmakers were criticised for their approach. The GDPR as an EU regulation also automatically supersedes any German national law. This would not apply for Ukraine. The GDPR would not be directly applicable to Ukraine. Therefore, Ukrainian law would need to show full compliance with the GDPR. The violation of data subject rights is further one of the most penalised violations under the GDPR (Article 83 of the GDPR).

3. Special categories of PD for the new UkrDPL

We strongly advise putting the list of sensitive data in line with the wording of the GDPR (please see above, under Part Two, Section 2.). Every potential amendment (also based on the national DPA guidance, e.g., localisation data to be sensitive data) would lead to legal uncertainty. We also suggest naming this category as sensitive personal data and amending the current wording accordingly (currently "high-risk data"). With regard to the legal basis for sensitive data processing, we recommend to include the list of legal grounds indicated in the Article 9 (2) of the GDPR²⁶⁸ with the following clarification of the applicability of the various legal grounds considering the data controllers role, function and the purpose of data processing. We further suggest including explicitly into the UkrDPL obligations (e.g., notification of the data subject and the national DPA) connected to a data breach incident with PD. With regard to a data breach connected to sensitive personal data, we suggest implementing a deadline of reporting to the data subject and the national DPA to stress the importance and possible damage connected to data breaches of sensitive data.

4. ADM prerequisites for the new UkrDPL

The GDPR compliance concerning ADM is also critical and a highly regulated topic in the GDPR. We suggest including the strict requirements of the GDPR into UkrDPL similar to the way it was reflected in the DPA 2018 and BDSG, also in the perspective of an EU adequacy decision. If the GDPR requirements are implemented in UkrDPL, no extra regulation concerning state authorities would be necessary.

5. Certification approach for the new UkrDPL

We don't see the necessity to implement a certification process under which companies (Ukrainian and foreign) can get certified to comply with Ukrainian law. The certification as an instrument to comply with GDPR standards for having a simpler way to transfer data from/to outside the EU is not necessary for Ukrainian reality. Ukrainian law does not have and should not have an extraterritorial effect (please see above). We further assume that the other cross-border transfer instruments as suggested above would be enough to simplify the cross-border transfer from Ukraine to outside.

In addition, when the new UkrDPL is adopted, its level of data protection will still not be formally adequate according to GDPR. Until obtaining the EU adequacy decision, the introduction of voluntary certification to comply with Ukrainian law will not be considered practically useful from the perspective of either Ukrainian or foreign businesses. Hence, such certification in the Ukrainian realities could be used solely as a competitive advantage (although we are convinced that certification under ISO standards would be considered a much stronger advantage due to its global nature).

Certification for other standards (e.g., ISO 27001 or GDPR) may be possible. However, based on our experience, the Ukrainian national authority for accreditation would not be able to implement a new certification process in Ukraine within the next years. Therefore, we suggest not to implement a GDPR

²⁶⁸ The Article 9 (2) provides legal grounds for sensitive data processing as the exemption from general prohibiting rule:

- (a) Explicit consent;
- (b) Employment, social security and social protection (if authorised by law);
- (c) Vital interests;
- (d) Not-for-profit bodies;
- (e) Made public by the data subject;
- (f) Legal claims or judicial acts;
- (g) Reasons of substantial public interest (with a basis in law);
- (h) Health or social care (with a basis in law);
- (i) Public health (with a basis in law); and
- (j) Archiving, research and statistics (with a basis in law).

certification process within Ukraine and not to apply before the EDPB to get formal recognition of certification schemes as a non-EU member. Such a certification scheme is also not necessary to obtain an EU adequacy decision.

However, if it is decided to implement the certification mechanism in Ukrainian law, it should be noted that there has been no similar mechanism in Ukraine, yet. The implementation of the concept, recruitment and professional development of relevant specialists, adoption of best practice of other jurisdictions regarding certification mechanism may be rather time-consuming. For instance, in the UK, the process of introducing the privacy seals was launched by ICO back in 2012, and the first certification schemes became operational by 2016 only.

Powers of new Ukrainian DPA

We would not recommend providing the new Ukrainian DPA with either accreditation (sole, or joint – German approach) or certification (French approach) powers. Excluding such powers from the new Ukrainian DPA should be more cost-efficient and will allow the DPA to concentrate mainly on its monitoring and mainly regulatory functions.

Similar to the EU approach, the new Ukrainian DPA should be empowered to issue some accreditation requirements additional to ISO 17065/2012 that are to be used by the national accreditation body, as well as certification criteria.

Accreditation body

We recommend appointing the National Accreditation Agency of Ukraine as an accreditation body in data protection matters. For this, it should be able to engage specialists with relevant data protection expertise.

In turn, it is also possible to follow the German scenario²⁶⁹ and provide the National Accreditation Agency with accreditation powers jointly with the new Ukrainian DPA. However, this may require additional amendments to the system of national accreditation and put additional burden on the new Ukrainian DPA. Therefore, we would not recommend implementing such an approach.

Given the EDPB general guidelines on accreditation requirements and experience of countries that already have such requirements in place, the certification body should meet at least the requirements set out, either in new UkrDPL or supplementary legislation, as follows:

- certification body demonstrates:
 - independence by way of providing separate evidence regarding its financing regarding the assurance of impartiality²⁷⁰; and
 - expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority (Article 43(2)(a));
- certification body demonstrates that its tasks and duties do not result in a conflict of interests (Article 43(2)(e));
- certification body has appropriate measures (e.g., insurance or reserves) to cover its liabilities²⁷¹;
- certification body has established:
 - procedures for the issuing, periodic review and withdrawal of data protection certification (Article 43(2)(c));
 - procedures to handle complaints about infringements of the certification where such procedures and are transparent to data subjects and the public (Article 43(2)(d));
- personnel of technical expertise should have:
 - a qualification in a relevant area of technical expertise;
 - significant professional experience in identifying and implementing data protection measures; and

²⁶⁹ Section 39, [BDSG](#).

²⁷⁰ Section 4.2, Annex 1, [Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation \(2016/679\) - Annex 1](#).

²⁷¹ Clause 4.3, [UK additional accreditation requirements for certification bodies \(A.43\(1\)\(b\)\)](#).

-
- significant relevant professional experience in technical data protection and knowledge and experience in relevant certifications/audits;
 - personnel of legal expertise should have:
 - a legal qualification from a reputable law school;
 - significant relevant professional experience in data protection law; and
 - relevant knowledge and experience in relevant certifications/audits²⁷²;
 - if engaging subcontractors for the certification, the certification body needs to ensure that the data protection expertise required for the accredited certification body must also be in place and demonstrated with the subcontractor with respect to the relevant activity performed²⁷³.

In order to ensure proper and comprehensive review and monitoring, the accreditation process should include four phases similar to the German law approach – application, assessment, accreditation and post-accreditation surveillance²⁷⁴. The accreditation shall be valid for no more than five (5) years (Article 43(4)).

Certification bodies

The current Ukrainian legislation allows both public and private companies to act as certifiers of services and processes. Using services of private certification companies should allow decreasing budgetary expenses for state support of the data protection system.

Given that German and UK authorities are in the process of developing their certification criteria yet, the certification criteria to be adopted by the new Ukrainian DPA should consider the respective EDPB guidelines²⁷⁵.

The certification criteria also need to take into account the specific needs of micro, small and medium-sized businesses (Article 42(1)). The certification should be issued for no more than three (3) years (Article 42(7)).

Supplementary legislation

Apart from adopting the new UkrDPL, we understand it will also be necessary to develop some secondary legislation covering the certification procedures and criteria, either by the new Ukrainian DPA or other state authorities. However, we suggest providing the new DPA with an active role in defining the necessary requirements for establishing and monitoring a process of certification.

6. Direct marketing approach for the new UkrDPL

We suggest implementing regulations and principles for direct marketing in the UkrDPL as outlined in the GDPR and the ePrivacy Directive. All of the compared non-EU laws also lean to the European standards in this regard. For legal security and competitive advantages for Ukrainian businesses, we suggest fully complying with the EU standards. It is also essential having additional guidelines on direct marketing published by the new Ukrainian DPA.

²⁷² Section 6.1, [UK additional accreditation requirements for certification bodies \(A.43\(1\)\(b\)\)](#).

²⁷³ Clause 47, [Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation \(2016/679\) - Annex 1](#).

²⁷⁴ <https://www.dakks.de/en/content/how-does-accreditation-procedure-work>

²⁷⁵ [Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation](#).