TUCA ZBARCEA
ASOCIATII

15 November 2019

Legal Alert

A selection of relevant EU developments as regards Data Privacy – October 2019

In this issue:

1. **National legislation related to Data Privacy**
2. **Sanctions for breach of GDPR**
3. **EU Official Guidelines and Standards**
4. **EU Jurisprudence**
5. **Our cherry**

LEGISLATION

Government Decision No. 584/2019 amending and supplementing Government Decision No. 494/2011 on the establishment of the National Cyber Security Incident Response Centre - CERT-RO

● Romania Gazette Part I No. 673 as of August 13, 2019. ● Date of entry into force: August 13, 2019 ● Applies from: August 27, 2019

The Decision regulated the establishment of CERT RO – as the competent authority at national level for the security of network and information systems providing essential services or providing digital services within the meaning of Law No. 362/2018.

NBR Regulation No. 2/2019 on preventing and combating money laundering and terrorist financing

● Romania Gazette Part I No. 736 as of September 9, 2019. ● Date of entry into force: September 9, 2019 ● Applies from: October 2, 2019

The Regulation changes the rules on client vetting. *Inter alia*, the following changes are notable:

- Provisions on data minimisation– e.g. for occasional transactions less data may be processed for vetting purposes; the possibility to apply simplified client vetting measures where there is a low risk for money laundering and terrorist financing;
- Credit institutions cannot initiate, continue a business relationship or carry out an occasional transaction if they do not put in place customer awareness measures, including in cases where they cannot establish the legitimacy of purpose and the nature of the business relationship or cannot manage the risk of money laundering and terrorist financing.

TUCA ZBARCEA
ASOCIATII

SANCTIONS FOR BREACH OF GDPR

AUTHORITY	FINE	INFRINGEMENT	INDUSTRY	NO. OF DATA SUBJECTS	HIGHLIGHTS
Romanian DPA (ANSPDCP)	EUR 150,000	Failure to take adequate technical and organizational measures for preventing unauthorized access and disclosure of personal data	Financial Services	1,177	/ The controller must ensure that the natural persons acting under its authority process the personal data within the limits of their job duties, and not for personal purposes (e.g., implementing internal rules for data management, implementing adequate controls for compliance with relevant internal rules).
	EUR 20,000	Unlawful disclosure of personal data Not notifying the data breach to the national supervisory authority	Financial Services	1,177	/ The controller must notify the personal data breach to supervisory authority without undue delay (and, where feasible, not later than 72 hours) after having become aware of it.
	EUR 9,000	Not being able to prove explicit consent Inadequate legal grounds	Online services	4,357	/ Consent should be given by a clear affirmative act. Collecting consent by silence (users who do not check the box stating I do not want to receive Personal Update) is not adequate. / Controllers should make sure adequate legal ground is used for the processing – e.g. sending a daily update on the articles posted on a news website does not fall under the need to perform a contract but requires data subjects' consent.
	EUR 2,100	Failure to consider data subjects unsubscribing (breach of Law No. 506/2004 rules)	Online services	1	/ Organizations must implement adequate controls to ensure receiving and implementation of consent withdrawal (e.g., adequately train employees, create dedicated withdrawal flows, dedicate a person for supervising management of withdrawal requests).
	EUR 1,000	Unlawful CCTV monitoring (breach of GDPR rules regarding transparency, data minimisation and lawfulness of processing).	Industrial furnace and heating equipment		/ Organizations should be able to prove that they have adequately informed the data subjects on CCTV monitoring.
Belgium DPA	EUR 10,000	Failure to comply with data minimisation principle - asking to read	Online commerce		/ Organizations must provide alternative options for access to a service, otherwise the consent is not deemed to be freely given.

			an electronic ID card as a condition for the provision of a service				
Polish DPA (UODO)		EUR 644,780	Inadequate organizational and technical safeguards that led to unauthorized access to the customer database of an online store	Online commerce	Approx. 2.2 mil.	/	The data shall be processed in a manner that ensures appropriate security of the personal data.
Polish DPA (UODO)		EUR 9,380	Not concluding an adequate agreement in line with Art. 28 of GDPR Failure to comply with storage limitation rules	Public institutions		/ /	Where the processing is carried out on a behalf of a controller by a processor, the processing shall be governed by a contract or other legal act that sets out the subject-matter and duration of processing, the nature and purpose of processing, the type of personal data (in the case at hand with the company offering storage services and the company providing software programs). The controller must carry a risk analysis and implement the appropriate security measures referred to in art. 32 of the GDPR, corresponding to the risk of violating the rights or freedoms of natural persons.
Spanish DPA (AEPD)		EUR 60,000	Unlawful processing of data by failure to identify data subject	Cosmetics	1	/	Controllers should deploy minimum diligence in order to verify the interlocutors to avoid unauthorized use of other individuals' identity.
		EUR 36,000	Unlawful processing of data by failure to identify data subject	Electronic communications services provider	1	/	Controllers should deploy minimum diligence in order to verify the interlocutors to avoid unauthorized use of other individuals' identity (in case at hand, the consent given by a family member of the data subject is not deemed valid for processing of family members data).
		EUR 30,000	No legal basis for not allowing refuse of cookies on a website	Aviation		/	Companies must provide a mechanism that allows the website user to manifest actively consent for different categories of cookies (granular access).
		EUR 8,000	Lack of cooperation with the supervisory authority	Electricity		/	Failure to provide DPAs with required information may lead to fines
Swedish DPA		EUR 18,630	Unlawful use of facial recognition technology in order to monitor the attendance of students	Education		/	In case of an existing relationship based on the dependency between the data subject and the controller, it is necessary to evaluate if the consent is an adequate basis for processing – the consent is not deemed to be freely given.

Norwegian DPA	EUR 49,100	Insufficient organizational and technical safeguards that led to unauthorized access to the personal data	Public Institution		/	Organizations must give access to personal data only to the employees that need it in order to perform their job duties.
Bulgarian DPA	EUR 2,600,000	Insufficient organizational and technical safeguards that led to online dissemination of a database	National Revenue Agency	Approx. 6 mil	/	In case of a cyber-attack, the controller must prove it had previously deployed adequate technical and organizational security measures in order to protect the personal data.
	EUR 511,000	Insufficient organizational and technical safeguards that led to dissemination of 23,000 credit records	Financial Services	33,000	/	Organizations must implement adequate technical and organizational security measures.
Latvian DPA	EUR 7,000	Not responding to the data subject's request to erase his personal data Not cooperating with the DPA	Online commerce		/ /	Organizations must implement a Data subject access/privacy requests procedure. The DPAs take in consideration when deciding on the amount of the fine, inter alia, of the degree of cooperation with the supervisory authority.
Austrian DPA	EUR 18,000,000	No legal basis for data processing	Austrian Post	Approx. 3 mil	/	Creating profiles for more than three million Austrians, which included information about their home addresses, personal preferences, habits and possible party affinity and selling the profiles for example to political parties and companies was deemed as not having a sufficient legal ground under Art. 6 of GDPR
	EUR 50,000	Not appointing a DPO when mandatory Wrongfully founding the processing on consent Not carrying a Data Protection Impact Assessment when mandatory	Medical Services		/	Organizations must verify if the processing requires appointing a DPO or a Data Protection Impact Assessment.
German DPA	EUR 14,500,000	Failure to comply with data minimisation principle	Real Estate		/	Organizations must restrict the personal data processed regarding the data subject in terms of period of time and categories of data to what is necessary for the purposes of processing (In case at hand, information regarding

						salary statements, self-disclosure forms, extracts from employment and training contracts, tax, social security and health insurance, bank statements of tenants shouldn't have been collected initially nor stored for a long period of time.).
	EUR 195,407	Sending commercial messages even if the data subject's account on the controller's website had not been active for a long period	Catering services	9	/	Organizations must implement a Data Retention Policy and erase personal data that exceed the storage period.
Greek DPA	EUR 200,000	Failure to consider data subjects unsubscribing from 3rd parties marketing	Electronic communications services provider		/	The data shall be processed in a manner that ensures appropriate security of the personal data and that ensures adequate management of opt-out requests.
	EUR 200,000	Non-compliance with right to object and data privacy by design and by default	Electronic communications services provider	8,000	/	The controller must implement adequate organizational and technical means to ensure exercise of right to object and erasure of data in such context.

GUIDELINES

When "time is of essence": ICO – recommendation of timescale for data subjects access requests (SARs)

Following the *CJEU ruling in Case C-171/03 Maatschap Toeters and M.C. Verberk Productschap Vee en Vleesof*, ICO *updated its guidance* on data subjects requests.

Highlights: Timescale for a SAR reply

/ When establishing the deadline for replying to SARs, the day of receipt of the SAR shall count as "Day 1". This means that the reply deadline to a SAR received on 29th of August is 29th of September (and NOT 30th of September).

/ Same timescale should apply for computing the reply deadline for the other data subjects' rights regulated under GDPR.

Ready? The Lower Saxony data protection authority ("LfD Niedersachsen") GDPR implementation checklist

LfD Niedersachsen published a GDPR implementation *checklist* which may be used to verify current GDPR compliance status.

IAB Tech Lab updates the technical specifications for the IAB Europe Transparency & Consent Framework

IAB Europe, the leading European-level industry association for the digital marketing and advertising ecosystem, in partnership with *IAB Tech Lab*, announced the launch of the second iteration of the *Transparency and Consent Framework (TCF)*.

DPO Handbook[1]

The handbook aims at supporting the training of data protection officers (DPOs) **for public institutions** in their new duties under the GDPR. Though addressed to public institutions, same standards could be considered in case of DPOs from **private sectors**. The handbook may be accessed ***here***.

Highlights:

[1] Issued by the following data protection authorities: Garante per la Protezione dei Dati Personali (Italy), Agencia de Proteccion de Datos (Spain), Agencija za zastitu osobnih podataka (Croatia), Commission for Personal Data Protection (Bulgaria) and Urząd Ochrony Danych Osobowych (Poland).

/ DPO's expert knowledge refers to:

(a) expertise in the area of EU privacy and data protection law, including expertise in IT and IT Security; and

(b) a good understanding of the way the institution [to which the DPO is appointed] operates and of its personal data processing activities, and an ability to interpret relevant data protection rules in that context.

/ Technical knowledge of IT systems implies a good understanding of the IT terminology, [IT] practices and different forms of processing of data. A DPO should be knowledgeable about, for example, data management and exploitation systems, types of software used, files and data storage systems, as well as about the requirements of confidentiality and security policies (data encryption, electronic signatures, biometrics, etc.

Schleswig-Holstein State Commissioner for Data Protection ("**ULD**") tips for security breaches prevention – German version available only

ULD published some *tips* for prevention of security breaches. *Inter alia*, it refers to the need to use encryption where your website displays forms for collection of customer data.

The Information Commissioner ("**IC**") of Isle of Man: Guidance on use of CCTV

IC has published a *guideline on CCTV use* by controllers.

Highlights:

/ CCTV cameras should be sited, and image capture restricted, to ensure that they do not cover areas not of interest or not intended to be monitored (such as individuals' private property).

/ The system must have the necessary technical specification to ensure that images are of the appropriate quality for the envisaged purpose.

/ CCTV camera signs/ pictograms should: (i) be clearly visible and readable; (ii) indicate details of the organization operating the system, the purpose(s) for using CCTV, and who to contact about the scheme - where not obvious depending on context ; and (iii) be of an appropriate size.

/ Disclosure of images from the video system must also be controlled and consistent with the purpose for which the system was established. However, individuals have the right to request copies of their images.

The Malta Gaming Authority: Commercial Communications Guideline

These Guidelines are aimed to provide practical guidance to any person offering licensable game/s and to persons which collaborate in any way or provide any service including any marketing or promotional service to or on behalf of such persons.

CNIL (French DPA) Statement: Recording of employees' phone conversations and computer actions

CNIL published a *statement* on recording of employees' telephones' and computers' actions (available only in French).

Highlights:

/ As a rule, screenshots coupled with recording of phone conversations is disproportionate when used for other purposes than training (e.g., staff evaluation, combating internal fraud, etc.)

AEPD (Spanish DPA) Technical Note: Proactive responsibility in mobile apps

AEPD published a *technical note* outlining GDPR practices for the organizations responsible for the processing on mobile application and the developers of such applications.

Highlights:

/ The GDPR information must be available both in the app store and in the application in a language appropriate to the target user;

/ The organisations controllers of the data in the applications must stipulate in the data processing agreements the processors' obligation to ensure good practices and consider privacy by design and by default from the very conception of the applications;

/ The following practices should be particularly considered: granularity in management of access permissions to protected system resources; respecting user's privacy preferences; don't disseminate data to analytics and advertising services from the moment the applications start, without the user to be able to make any use or adjustments; use advanced methods for communications encryption.

Garante (Italian DPA): Code of conduct on credit risk analysis for private informative systems

Highlights:

/ The processing of personal data contained in a SIC can be carried out exclusively for purposes related to the evaluation, recruitment or management of a credit risk, to the assessment of reliability and punctuality in the payments of the interested party – in view of preventing the risk of fraud and identity theft;

/ The processing of personal data is necessary for the pursuit of legitimate interests of the participants in the use of the SIC for the purposes referred to in the CoC;

/ Negative credit information relating to late payments, subsequently regularized, can be kept in a SIC up to: a) twelve months from the date of registration of data relating to the regularization of delays not exceeding two instalments or months; b) twenty-four months from the date of registration of data relating to the regularization of delays exceeding two instalments or months.

EU JURISPRUDENCE

CJEU Decision on Google vs. CNIL

CJEU decided on 24 September 2019 that when receiving a request for de-referencing made by a data subject pursuant to GDPR, the operator of the search engine is not required to carry out the de-referencing on all version of such engine, but only on those version corresponding to all EU Member States.

CJEU Preliminary ruling on Article 15 (1) of Directive 2000/31/EC

CJEU issues on 3rd October 2019 a *preliminary ruling* on the interpretation of Article 15 (1) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce')

Highlights:

/ It decided that Directive on electronic commerce, in particular Article 15(1), must be interpreted as meaning that it does not preclude a court of a Member State from:

/ Ordering a host provider to remove information which it stores, the content of which is identical to the content of information, which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;

/ Ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, and

/ Ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.

OUR CHERRY

Future job opportunities for candidates

If the candidate is not selected for the next stage of the recruitment process, you might consider the following:

/ Inform the candidates clearly and completely before submitting their application on the manner in which their data is to be used for recruiting purposes.

/ Particularly:

(a) Let the candidates know if you intend to use their application also for other job positions than indicated in the recruitment announcement.

(b) Inform the candidates on their right to oppose without justification to the further use of their application for other available job positions. Be aware that the candidates might express their opposition also indirectly, for instance by specifically saying that they are only interested in the advertised position or by indicating the targeted job position.

/ If you intend to use the application for further job opportunities:

(a) Inform the candidates about such intention; particularly, indicate the applicable period for such further use and the safeguards you will take in this context (e.g., inactive storage – such as archiving, pseudonymisation/ encryption, limited access, etc.); and
(b) Obtain the candidates' consent for such use.

Editors

Țuca Zbârcea & Asociatii has an all-embracing experience in providing legal advice in the area of data privacy/ GDPR to top companies in Romania and/or abroad, active in various commercial sectors, such as: telecom, financial services (banking, insurance, pensions, etc.), healthcare, pharmacy, e-commerce, IT, energy, food supply, etc.

The legal assistance provided covers all aspects of data privacy, from legal assistance before the local regulatory authority (The National Supervisory Authority for Personal Data Processing – **ANSPDCP**) in relation to various issues (such as notification of personal data breaches, consultation for high risk data protection impact assessments, consultation on sensitive legitimate interest assessments, etc.) to complex legal assistance in the field of data privacy/ GDPR, such as: full GDPR implementation; carrying out data privacy impact assessments (DPIAs) and legitimate interests assessments (LIAs); employee monitoring, geolocation, call history; cookies; cloud computing solutions; auditing of data processors; personal data sharing; negotiation of relevant terms of data processing agreements (DPAs); industry codes of conducts; GDPR/ data privacy trainings; handling of data subjects' complaints, etc. For further information and other recent news relating to Data Privacy, please feel free to visit our firm's blog – *dataprivacyblog.tuca.ro*

Horia Ispas
Partner
+40 37 413 63 16
horia.ispas@tuca.ro

Ciprian Timofte
Managing Associate
+4 021 204 88 90
ciprian.timofte@tuca.ro

TUCA ZBARCEA
ASOCIATII

Șos. Nicolae Titulescu nr. 4-8
America House, Aripa de Vest, et. 8
Sector 1, 011141, București, România
T + 4 021 204 88 90
F + 4 021 204 88 99
E office@tuca.ro
www.tuca.ro