Cloud Computing Data Protection Aspects under Croatian and European Union Law

Nina Gumzej
Chair of Legal Informatics
University of Zagreb Faculty of Law
Zagreb, Croatia
nina.gumzej@pravo.hr

Dražen Dragičević
Chair of Legal Informatics
University of Zagreb Faculty of Law
Zagreb, Croatia
drazen@pravo.hr

***Abstract*— In the introduction authors explain recent developments with regard to regulation of personal data protection aspects of cloud computing services at European Union level. This is followed by analysis of the relevant EU legal framework and interpretations on its application to data processing in the context of cloud computing, and of the data protection legal framework of the Republic of Croatia and guidance on data protection in cloud computing issued by the relevant regulatory authority, *i.e.* Personal Data Protection Agency. Authors next examine proposed new EU general data protection framework that is currently in legislative process (Proposal for General Data Protection Regulation). This research focuses on selected provisions of the most recent draft text adopted by the European Parliament (amending the 2012 Commission's original proposal) that are likely to significantly impact the EU cloud computing market. Authors conclude overall analysis in the paper with assessment of likely impacts of analyzed solutions for cloud computing clients and providers, and in relation to legislation that is currently in force. While estimating that relevant legislation and practice in Croatia will further develop in line with the EU framework, research in this paper aims to more generally contribute to development of domestic legal writing in the area and to the raising of public awareness on legal data protection issues that need to be considered when switching to the cloud.**

Keywords—cloud computing; personal data protection; Personal Data Protection Act; General Data Protection Regulation

I. INTRODUCTION

According to the widely used definition of the National Institute of Standards and Technology of the U.S. Department of Commerce (NIST), cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. As such the cloud computing service is characterized by five key elements (on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service), three service models (Software as a Service - SaaS, Platform as a Service - PaaS, Infrastructure as a Service - IaaS) and four models of deployment (private, communal, public and hybrid cloud) [1]. Described virtualization can provide many benefits for cloud clients (users, customers) especially in terms of savings, meaning they can benefit from opportunities for optimization of their business without investing the otherwise significant resources (depending on particular model) in the development and maintenance of relevant infrastructure and IT systems.

In 2012 the European Commission adopted the strategy "Unleashing the potential of cloud computing in Europe" (further also as: Cloud Computing Strategy) [2] where it acknowledges the many social and economic benefits of cloud computing at EU level, in particular through increased GDP growth and creation of new jobs. Later on the Commission initiated and financially supported the *European Cloud Partnership* towards common standards for public procurement. A lot of effort has so far also been invested into ensuring elementary technical conditions and standardization (interoperability, service portability). Certainly, the often complex architecture of cloud computing services and terms of their provisioning raises many other issues that need to be resolved, including the issue on ensuring security of data in the cloud while acknowledging the risks associated with virtualization of IT infrastructure and systems. Without prejudice to work of others we would in that respect point in particular to activities of the *European Union Agency for Network and Information Security* (ENISA) and reports with valuable advice and recommendations for stakeholders [3].

When considering application of the law in the cloud computing context it must first be noted that this may entail application of diverse legal areas, including but not limited to areas of information security and cybersecurity, consumer protection law, contract and intellectual property law, electronic commerce and electronic identification and trust in electronic transactions. In this paper, however, we will focus only on legal issues with respect to processing of personal data in cloud computing (under EU data protection law the term *personal data* denotes any information relating to identified or identifiable natural person, *i.e.* data subject and the term *processing* denotes a broad range of operations that can be performed on them, such as collection, copying, storage, erasure).[1] We were prompted for this research in particular due to the fact that privacy and security of personal data

[1] For more details see Articles 2(a)-2(b) as well as recital 26 of "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", Official Journal of the European Union L 281, 23. 11. 1995, pp. 31–50 (General Data Protection Directive).

(further also as: data) was one of the main concerns reported by stakeholders in consultations preceding Commission's adoption of its Cloud Computing Strategy. In particular noted was lacking clarity in interpretation and application of a number of important aspects of cloud computing in terms of data protection legislation, e.g. applicable law, roles of different players (including the corresponding responsibility and liability issues) and cross-border data transfers. This is in particular highlighted by diverse national law solutions despite their common EU base (*Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, further as: General Data Protection Directive or Directive) [4]. To address these concerns the Commission announced on one side future work on establishing model contract terms and conditions covering issues such as preservation of data after contract termination, change of service by providers, subcontracting, disclosure, location, transfer, integrity and ownership of the data. In particular, Commission anticipates earlier mentioned concerns would properly be addressed by solutions of the proposed new EU general data protection legal framework (further as: *General Data Protection Regulation* or *Regulation*) [5] that is to replace the Directive, most probably with the support of additional instruments towards interpretation of application of these new rules specifically to the cloud computing context. We will address relevant solutions of the Regulation in section IV of this paper. Until adoption of this new framework, which is at the moment still in legislative process, Commission referred to available expert guidance, in particular that of the EU independent advisory body *Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data* (further as: Art. 29 WP).[2] Namely, in 2012 the Art. 29 WP issued an opinion with detailed interpretations on applicability of the current EU data protection framework in cloud computing, in which it acknowledged *lack of control over the data and of information on their processing* as main groups of risks [6]. In the next section we will examine selected points of this opinion that are especially important for the topic of this paper. It goes without saying that all these developments directly concern the evolving cloud computing market and research on this and related areas in Croatia [7].

Structure of this paper is as follows. After introduction we will provide an overview of current EU general data protection legal framework, with an emphasis on interpretations, guidance and recommendations on its proper application in the cloud computing context. Next we will explain the relevant legal framework in Croatia, while focusing especially on relevant guidance and recommendations provided by the national data protection authority. In the fourth section we will examine selected provisions of proposed General Data Protection Regulation so as to evaluate its impact toward resolving identified problematic issues according to the current EU framework. In the conclusion we will appraise results of research in the paper and provide recommendations in particular with respect to enhancing public awareness and transparency on this topic in Croatia.

[2] It was established by Article 29 of the General Data Protection Directive and is composed of representatives of EU Member States' data protection authorities, European Data Protection Supervisor and European Commission's representative. Its documents are not legally binding, but can be considered authoritative, see e.g. C. Kuner, "European data protection law - corporate compliance and regulation", 2nd ed., Oxford University Press, 2007, at p. 10. (point 1.19.).

II. PERSONAL DATA PROCESSING IN CLOUD COMPUTING AND THE CURRENT EU FRAMEWORK

As noted in the previous section, General Data Protection Directive is the currently valid act governing general personal data protection at EU level. The Directive is technologically neutral and it applies as such also to personal data processing in the cloud computing context. It is primarily important to point to the concepts of *controller* and *processor*, with which the role and corresponding responsibilities of relevant players in the cloud computing eco-system are defined pursuant to applicable data protection rules based on the Directive. Namely, *controller* is main responsible actor for compliance with data protection obligations, as it determines (on its own or jointly with others) *purposes and means* of data processing. Controllers are bound by many data protection obligations, e.g. implementation of relevant data protection measures, as well as by fundamental requirements such as to process personal data fairly and lawfully, collect them for a purpose known to the data subject that is explicit and in accordance with the law, and further process them only for the purpose they were collected (or one corresponding to it). They are also not allowed to process the data that are not relevant for a specified purpose and process them beyond that what is necessary to achieve it. Furthermore, controllers are prohibited from keeping the data longer than necessary to achieve the purpose for which they were collected or further processed (certain exceptions can apply to these rules, but we will not discuss them in this paper). Controllers need to be clearly distinguished from *processors*, who merely process the data on their behalf and upon their instructions.[3] While controllers are according to the Directive main responsible (and liable) parties for ensuring compliance with applicable data protection rules, processors have only limited obligations as those who process data on behalf of controllers. This is also evident from solutions on liability for damages that the data subjects incurred due to breaches of relevant data protection rules. Namely, unlike for controllers, such liability towards data subjects is not established also for processors. This also means that where the processor violates relevant rules in such cases (and damages are incurred), matters such as compensation of damages need to be regulated in a legal act governing its relationship with the controller.

Directive also stipulates special obligations in cases where the controller decides to assign all or some of its data processing activities to the processor. These include a duty to only choose the processor providing sufficient guarantees on security measures with respect to data processing and ensuring compliance with them. Furthermore, controller and processor must have established legal relationship (concluded contract or other legal act by which the processor is bound to the controller). It must especially be specified, in writing or equivalent form, that the processor only acts on controller's instructions and that it is bound by the duty to ensure technical and organizational data protection measures.

Identification of controller and processor needs to be assessed on a case-by-case basis, e.g. so as to establish the *degree of control* over personal data processing and this may

[3] Article 2 points (d)-(e) of the General Data Protection Directive.

also vary, such as for example, where use of service includes several different data processing stages. Furthermore, some commentators also argue a need to acknowledge providers' *neutral intermediary role* (e.g. for pure infrastructure providers), in particular with respect to the degree of their (non-)influence over relevant processing of the data [8]. So far a number of commentators addressed practical difficulties in establishing roles of different actors in modern complex data processing environments in accordance with traditional, clear-cut data protection concepts of the controller and processor, in particular in relation to more complex cloud computing systems comprising different architectural layers [9]. According to the Cloud Computing Strategy, these and other concerns identified and brought to Commission' attention in relation to application of the Directive in the context of cloud computing are to be resolved with adoption of the Regulation (which we will examine in section IV). In that respect, however, expert opinions on further room for improvement in the Regulation, in particular towards better clarity should here also be noted [10]. As for interpretations of application of the current EU data protection framework in cloud computing, we will next examine, in reference to earlier mentioned Commission's noting of Art. 29 WP's work in that respect, selected aspects of this body's Opinion on Cloud Computing. In its opinion, Art. 29 WP highlights importance of appropriate establishment of roles that various cloud computing players have in order to properly determine their respective data protection duties. Its analysis is primarily based on the General Data Protection Directive as the generally applicable framework for personal data processing in connection with the provision of cloud computing services.

In interpreting duties and responsibilities of cloud clients and providers, Art. 29 WP focuses on situations where the provider acts as a processor of personal data on behalf of the client, who establishes the ultimate purpose of processing and decides on outsourcing of this processing and delegation of all or part of the processing activities. In such cases clients would assume controller's role and they would be fully responsible for compliance with applicable data protection obligations. Clients may entrust cloud providers with the choice of methods and technical measures that are to be used for accomplishment of controller's purposes, and as such the providers are considered to be processors, when they provide the means and platform on behalf of the client. However, roles must be established on a case-by-case basis, *i.e.* on the basis of facts of each particular case and in accordance with the earlier mentioned definitions of the controller and processor. In that sense the Art. 29 WP clarified that in some cases cloud providers could be considered as *joint controllers, or even controllers on their own* (e.g. when they process the data for their own purposes). Furthermore, in certain cases, where individual end-users use social networking services, providers of such services are considered the controllers (who determine purposes and means of processing the data, which the users publish and exchange with others).[4] In any case, when cloud providers do act as processors, clients must in their role of the controller observe all duties and remain responsible for acting in compliance with the applicable data protection rules. This also applies in situations where cloud clients are asked to accept or adhere to providers' standardized terms and conditions with respect to data processing. Namely, clients are not for this reason absolved of their responsibility to ensure compliance of relevant data processing with the rules, and this is why they must only choose providers guaranteeing compliance with those rules. Consequently, Art. 29 WP provides a number of details on the contractual relationship between the controller (cloud client) and processor (cloud provider) and points to be included that are specifically pertinent for the cloud computing data processing context. Primarily, fundamental data protection principles must be ensured: transparency on data processing, purpose specification and limitation principle, as well as the principle of data erasure. Details that should be regulated in contracts (contractual safeguards) include information on personal data processing and client's instructions to the provider; provider's security measures (details on technical and organizational measures of data protection and security that should be included in contracts so as to ensure the goals of *availability*, *confidentiality*, *integrity*, *transparency*, *isolation*, *i.e.* purpose limitation, *intervenability*, *i.e.* provider's support for data subjects' exercise of their data protection rights, *accountability* and *data and service portability*); details on provider's duties (e.g. support to clients in exercising their data protection rights); prohibited transfers of the data to third parties (with the exception of possibly engaged subcontractors with client's prior consent); duty to provide information on all possible data processing locations; logging and auditing of data processing (by the provider or subcontractors); statement on client's right to monitor and on provider's cooperation with the client to that effect; details on conditions of returning or destroying the data (including the secure erasure at client's request) after end of service; details on the duty to notify the client on personal data breaches, as well as on requests to disclose the data to law enforcement bodies, where permitted; provider's general statement on its overall organizational compliance (and its subcontractor, if any) with relevant legislation and standards, and the duty to inform the client on changes to the service.

Fundamental transparency principle requires that the provider informs the client of any subcontractors engaged in data processing. In that respect it is important to note that where the provider decides to engage a subcontractor, *i.e.* sub-processor (where the provider acts as processor) for the provision of its service, it can pursuant to the Art. 29 WP *only do so with prior client's consent.* In other words, this issue should be clearly stipulated in the relevant contract, as well as client's right to terminate it should there be changes in respect of this (provider must inform the client of these changes beforehand). Furthermore, provider should have concluded a contract with the subcontractor(s) containing all relevant data protection duties that it has towards the client (in provider's role of a processor) according to the main contract concluded with the client (controller). In the latter contract it should be ensured that the provider remains fully liable to the client where its subcontractor violates its data protection duties. Details on responsibility and liability need to in any case be contractually regulated between provider and subcontractor(s).

[4] For details (also on the issue of possible application of the so-called household exception to end-users publishing third party personal data), see: Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking", 01189/09/EN, WP 163, 12.6.2009, esp. at pp. 5-7; "Opinion 1/2010 on the concepts of "controller" and "processor"", 00264/10/EN, WP 169, 16.2.2010, esp. at p. 21.

Another important component of the earlier mentioned transparency requirement toward clients in cloud computing contracts according to Art. 29 WP also includes the duty to inform them on *all possible data processing locations*. This is important because, as mentioned earlier, clients remain responsible for data processing (as controllers in analyzed scenario with the provider acting as processor) and they must be able to assess if by agreeing to provider's contractual terms they are not in breach of applicable data protection legislation. Such possible violations can, for example, take place where the data are transferred outside the EU to third countries without adequate data protection levels [11]. In such cases several safeguards could be used in the cloud computing context, such as the *EU standard contractual clauses* [12] and *binding corporate rules* [13]. Art. 29 WP also discusses the *Safe Harbor* mechanism (for cases when the data are transferred outside the EU to the U.S.) [14], and warns that clients exporting the data should not simply rely on self-certification statements provided by U.S. companies to which the data are to be transferred. In other words, clients should carry out further checks on this. Where providers act as processors (and they are established outside the EU) the Art. 29 WP recommends the use of *Standard Contractual Clauses 2010/87/EU*, both in relationships between provider (acting as processor) and client (acting as controller) and between provider and its subcontractor(s) [15]. In connection with this it is useful to note that the Art. 29 WP recently established compliance of Microsoft's contract provisions for enterprise cloud services with the requirements on international data transfers from the mentioned EU clauses [16].

III. PERSONAL DATA PROTECTION ISSUES IN CLOUD COMPUTING AND THE CROATIAN LEGAL-REGULATORY FRAMEWORK

Croatia implemented the General Data Protection Directive in its *Personal Data Protection Act* (further also as: Act) [17]. To be noted in light of analysis in previous section is that unlike in the Directive, definition of controller in the Act does not explicitly include possible joint determination of purposes and means of data processing (multiple controllers). This notwithstanding, and despite the fact we found no relevant domestic case law or regulatory guidance, we do not consider that the mentioned lacking notion in the Act would impair potential application of the concept of multiple controllers in cloud computing also in domestic context.

In consideration of the relationship between the controller and processer it should be noted that mainly in line with the General Data Protection Directive (with minor differences in transposition, which we do not consider especially relevant and will not discuss here), the Act stipulates that the controller can only engage a processor who is registered for these activities and who provides sufficient guarantees as to implementation of appropriate data protection measures (and, where applicable, classified data protection measures in accordance with legislation on information security). In line with the Directive, controller and processor must regulate their mutual rights and obligations in a written contract. Controller must in particular oblige the processor to act only pursuant to its orders, not to provide the data to other users or process them for any other purpose than that defined by the contract, and to ensure appropriate (technical, organizational and staffing) data protection measures. To be noted in cases where sensitive personal data - special categories of personal data are processed (e.g. health data) is the special governmental act regulating their protection (*Regulation on the procedure for storage and special measures relating to the technical protection of special categories of personal data*) [18], which relies on ISO standards 27001 and 17799 (27002).

Until today many data protection supervisory authorities in Europe adopted some forms of guidance and recommendations on the topic of data protection and cloud computing (e.g. in Germany, Slovenia, Sweden, Italy, Spain, Czech Republic, the UK, France) [19]. The *Croatian Personal Data Protection Agency* (further also as: Agency) issued its guidance in 2012 [20]. From this guidance it can be deduced that in terms of establishing data protection roles and corresponding responsibilities the Agency mainly considers cloud providers as processors, and clients as controllers.

With respect to contracting cloud computing services the Agency advises that contracts with general terms and conditions should be avoided, as well as possibility of their unilateral amendment. This advice addresses primarily the need to insist on privacy protection and implementation of appropriate protection measures. Also, contracts should include an option that the controller (client) has the right to annul the contract in case of provider's amendment as well as the right to transfer the data to another provider. Furthermore, the Agency advises that controllers carry out *risk assessments prior to use of the cloud computing service*, on the basis of insight into specific conditions under which the data would be processed. That should include all locations where the data would be stored or processed in other ways (providers should in that respect ensure transparency, and the controllers should be in the position to inspect them). Controllers are also advised that in contracting with the provider they make in advance a complete list of information on all physical locations where the provider can store and process the data, during the contract period (including information on backup - principle of location transparency). Furthermore, the contract should clearly state that the data would not be transferred to other locations (beyond the list), irrespective of reasons for it and implemented protection measures. Cloud clients are also instructed to consider the need for ensuring access to at least one copy of the data beyond provider's control, which should be available to them (regardless of the provider).

According to the Agency cloud providers should develop practices to offer the highest possible transparency, security, responsibility and trust in cloud computing, particularly in relation to information on potential breaches and this should be supported by contractual solutions promoting users' enhanced control over the data (including, amongst others, providers' duty to report unauthorized access in 24 hours). The Agency also acknowledges the need for investing more effort in *certification mechanisms* as well as for implementation of the *privacy by design* principle towards increasing trust in cloud computing services. Furthermore, it notes that cloud providers should follow best practices and allow impartial third parties (auditors) to regularly conduct *risk assessments and impacts on personal data protection*.

Namely, it considers that mere possibility of providers' collection of large amounts of personal data should lead to regular checks by auditors, who should pay special attention to security aspects of data processing. Audits should check if the following functionalities are in place and in proper function: measures to prevent disallowed data transfers to subjects/entities without sufficient protection levels, or to subjects/entities not explicitly agreed to with the controller; measures to ensure detection of above stated activities; automated logging of records on the physical location where and when the data processing took place; automated logging of copying and erasing records; delete function providing for effective data erasure (e.g. momentary rewrite with random data) and automated access logging. The Agency also notes that personal data processed by way of information, communication and technical infrastructure should be protected in compliance with organizational security policy and with use of best practices and methodologies, such as the international standard ISO 27001. It considers implementation of standards as the clearest indication that measures are taken to protect the data, as well as a certain guarantee in terms of achieving appropriate technical, organizational and staffing data protection measures. Benefits of implementation and especially certification according to the ISO 27001 norm would come to the forefront when contracting cloud computing services, where that would be one of the important indicators on implemented data security controls.

IV. PROPOSED DATA PROTECTION REGULATION AND CLOUD COMPUTING

In this section we will examine selected provisions of the proposed General Data Protection Regulation according to the current draft text that includes the recently adopted amendments by the European Parliament (to the European Commission's proposal from 2012).[5] According to Commission's proposal as well as the current draft text, new legal framework is to be adopted in legal form of a regulation. Unlike directives, regulations are binding in entirety and they are directly applicable in all Member States. Therefore, adoption of the new framework as a regulation presents obvious benefits for cloud providers conducting data processing operations in more than one Member State (as well as for EU clients) in relation to the current situation that is characterized by diverse national solutions EU-wide implemented on the basis of the General Data Protection Directive. Regulation would not, however, entirely regulate all issues. Namely, in certain areas Member States would have discretion to pass national rules specially regulating some of the areas (under the conditions stipulated in the Regulation), such as e.g. in cases where data protection right conflicts with the right to freedom of expression.[6] Member States would also have a certain level of discretion in passing national rules regulating personal data processing issues in areas such as health, employment and social security, but also only under the conditions stipulated in the Regulation.[7]

Another important benefit for cloud providers lays in the proposed solution that their relevant data processing activities in all Member States are only subject to supervision by one authority, *i.e.* supervisory authority of their main establishment (*lead authority*). This would apply in all cases where controllers and processors are established in several Member States or where they process personal data of residents of several Member States.[8]

Similarly as today under the Directive, draft Regulation excludes certain areas from its otherwise general material scope of application, e.g. data processing by public authorities in the criminal law area (prevention, investigation, detection and prosecution of criminal offences, execution of criminal penalties). Also excluded from its scope is personal data processing by natural persons in the course of exclusively personal or household activity. While such exclusion is now also envisaged in the Directive, pursuant to draft Regulation this would apply in cases of processing that entails publication of personal data solely *where it can reasonably be expected that only a limited number of persons would access it.*[9] In other words it is proposed that the Regulation nonetheless applies if an individual publishes personal data openly for the public, e.g. online, without implemented access restrictions/limitations.[10] Furthermore, according to relevant recitals, in cases where this exemption applies, controllers and processors who *provide the means for processing personal data* for mentioned personal and domestic activities would still be subject to the Regulation. This would e.g. be the case of social networking providers.[11]

Proposed Regulation would have wide territorial scope. Namely, it would apply not only to data processing in the context of activities of controller's or processor's establishment in the Union (regardless of processing location, *i.e.* within or outside the EU), but also where controllers or processors without establishment in the EU process personal data of data subjects in the EU should processing operations relate to the offering of goods or services to them or to their monitoring. Therefore, under mentioned conditions, Regulation would also apply to non-EU cloud providers.[12]

As to fundamental data protection concepts, it should be noted that proposed new definition of personal data has been extended to also include identifiers such as location data and unique identifiers. Additionally, explanations in the relevant

[5] Note: further references to articles and recitals are therefore primarily made to the current draft text: "European Parliament legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)), P7_TA(2014)0212, Strasbourg, 12. 3. 2014. Where appropriate, *i.e.* for the purpose of comparing differences in proposed solutions, we will also refer the reader to original Commission's Proposal from 2012. For available analyses of Regulation specifically addressing the cloud computing context, see e.g.: I. S. Nwankwo, "Missing links in the proposed EU Data Protection Regulation and cloud computing scenarios: a brief overview", Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 5, issue 1, 2014, pp. 32-38, available at: https://www.jipitec.eu/issues/jipitec-5-1-2014/3905/jipitec_5_1_nwanko.pdf; W. K. Hon, E. Kosta, C. Millard, D. Stefanatou, "Cloud accountability: the likely impact of the proposed EU Data Protection Regulation", Queen Mary School of Law Legal Studies Research Paper No. 172/2014; Tilburg Law School Research Paper No. 07/2014, available at SSRN: http://ssrn.com/abstract=2405971.

[6] Article 80 of current draft text.

[7] Articles 81-82 of current draft text.

[8] For more details see Article 54a and Article 4 paragraph 13 of current draft text.

[9] For details on material scope of application, see Article 2 (compare with Commission's Proposal).

[10] For interpretation of the household exception according to General Data Protection Directive in relation to publication of personal data online, see: C-101/01, "Criminal proceedings against Bodil Lindqvist", Reports of Cases 2003 I-12971 (ECLI:EU:C:2003:596).

[11] Recital 15 of current draft text (compare with Commission's Proposal). For interpretations, see especially: European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"", Brussels, 16.11. 2012, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf at pp. 9-10.

[12] For more details on proposed territorial scope of application, see Article 3 of current draft text (compare with Commission's Proposal).

recital specify that the Regulation should apply to the processing that includes identifiers such as the IP addresses, cookie identifiers and RFID tags (unless these do not relate to identified or identifiable natural persons). Furthermore, draft Regulation introduces *pseudonymous* and *encrypted* data as new categories of personal data. The former are proposed to be defined as personal data that cannot be attributed to a specific data subject without using additional information, as long as that information is kept separately and subject to technical and organizational measures to ensure non-attribution. Encrypted data are defined as personal data made unintelligible by technological protection measures to all persons who are not authorized to access them.[13]

Current draft text of Regulation aims to more clearly allocate responsibilities and liabilities of all those who are effectively in charge of data processing[14], which is important in particular in more complex data processing environments such as that of cloud computing[15] (as explained earlier such responsibility is under the Directive mainly attributed only to the controller). Definitions of controllers and processors would remain essentially the same as in the Directive.[16] However, draft text of Regulation also explicitly introduces data processing circumstances with *joint controllers*, *i.e.* two or more controllers who jointly establish purposes and means of data processing. In that respect it should be noted additionally to earlier discussed interpretations of roles of cloud computing parties under the Directive, that the European Data Protection Supervisor acknowledged, specifically in relation to the proposed new EU framework and in the context of Cloud Computing Strategy, that in a number of cases cloud providers should be considered joint controllers or co-controllers (together with the client), rather than processors. This is so in particular due to clients' very limited level of control over data processing means, *i.e.* type of service offered (e.g. in cases of SaaS solutions such as cloud-based office productivity tools or business intelligence tools) [21]. In fact, due to increasing difficulties in establishing clear distinctions of different data processing roles in more complex digital processing surroundings, some commentators even propose that the processor concept is removed from draft Regulation and that all parties processing the data are considered controllers with attributed corresponding responsibilities for their processing activities [22].

In order to ensure effective allocation of responsibilities in mentioned joint controllership situations, draft Regulation stipulates the duty of joint controllers to *mutually arrange their respective responsibilities* for compliance with data protection duties, including their effective roles and relationships toward data subjects and especially as to procedures and mechanisms for exercising data subjects' rights. Additionally, it is specified that should these issues not be clearly arranged between them, joint controllers would be subject by default to the joint and several liability regime.[17] Also important new solution relevant in the cloud computing context addresses those situations where *processors process data beyond controller's instructions*, or *where they become determining parties in relation to purposes and means of data processing*. In such cases it is proposed that processors become bound by the applicable legal regime for joint controllers (with respect to relevant processing operations).[18]

Clearer attribution of responsibilities for all those who are effectively in charge of data processing has also resulted in more extensive data protection duties in draft Regulation for processors, such as the duty to keep and maintain documentation on personal data processing[19], duty to co-operate with the supervisory authority[20], as well as the duty to appoint a data protection officer.[21] Described new elements for allocation of responsibility as well as a set of reinforced obligations on the part of processors are also reflected in the proposed liability regime for damages. A person suffering damages due to unlawful processing or other action in contravention of the Regulation would have the right to receive compensation from the controller, or the processor.[22] Additionally, right to judicial remedy would be available also against the processor, and thus not only against the controller as currently prescribed in the Directive. These proceedings can be brought before courts of their (controllers' or processors') establishment, but also before the court of the Member State where the data subject has habitual residence.[23]

Controller who intends to assign data processing to the processor is only allowed to do so by choosing a processor demonstrating sufficient guarantees to implement appropriate technical and organizational measures and procedures so that the processing complies with the Regulation, and who ensures protection of data subjects' rights. This echoes the current solution in the Directive as does the duty to have their mutual relationship governed by a contract or other legal act that binds the processor to the controller. However, interestingly, draft Regulation also stipulates a possibility that the processors demonstrate mentioned guarantees if they adhere to the relevant *codes of conduct* and *certification mechanisms*. Namely, draft Regulation encourages development of codes of conduct specifying its application in particular sectors, such as the cloud computing sector. This reflects the today already envisaged support for the drafting and use of codes of conduct in the Directive. In relation to implementation of the Cloud Computing Strategy, and specifically Commission's action point to develop relevant code(s) of conduct together with the industry, is it important to keep track of developments on recently drafted *code of conduct for cloud computing providers* by the Cloud Select Industry Group on Code of Conduct, which has been submitted to the Art. 29 WP [23] (according to the Directive codes intended to apply at EU level may be submitted to the Art. 29 WP for approval). As for certification mechanisms, it is important to point to new solutions according to which both the controllers and processors may ask any supervisory authority in the EU to certify compliance of their data processing with the Regulation. Following successful certification they would receive a standardized mark (*European Data Protection Seal*).

[13] For more details see Article 4, paragraphs 2-2b as well as Recital 24 of current draft text (compare with Articles 1-2 and recital 24 in Commission's Proposal).
[14] Recital 62 current draft text (compare with Commission's Proposal).
[15] See e.g. Art. 29 WP Opinion 1/2010 on the issue, *supra* note 4.
[16] Article 4, paragraphs 5-6 of current draft text (compare with Commission's Proposal).
[17] Article 24 and Article 77 paragraph 2 of current draft text (compare with Commission's Proposal).
[18] Article 26 paragraph 4 of current draft text (compare with Commission's Proposal).
[19] For more details, see Article 28 of current draft text (compare with Commission's Proposal).
[20] Article 29 of current draft text.
[21] For more details see Articles 35-37 of current draft text (compare with Commission's Proposal).
[22] Article 77 of current draft text.
[23] Article 75 of current draft text.

Draft Regulation provides many more details than the Directive on obligatory contents of the mentioned contract or other legal act governing the controller-processor relationship. As a rule the following must be stipulated in writing as processor's obligation: processing the data only on controller's instructions (which must be documented in writing) and employing only the staff that is committed to confidentiality; taking all required measures on security of processing; establishing conditions to enlist another processor only with controller's prior permission, and determining in agreement with the controller technical and organizational requirements for fulfillment of controller's duty to respond to data subject's rights, as well as helping the controller to ensure compliance with certain duties (relating to security of processing, personal data breaches, conduct of risk analysis as to potential impact of processing on data subjects' rights and freedoms, as well as conduct of impact assessments, compliance reviews and prior consultations). Additionally, this legal act must envisage processor's duty to return all results to the controller after end of processing, not to process the data otherwise and to delete any copies thereof, as well as the duty to allow on-site inspections and provide the controller with all necessary information to prove compliance with its obligations.

Another very important newly introduced duty, that will be particularly relevant in the cloud computing context is the duty of both the controllers and processors to apply technical and organizational measures and procedures necessary to ensure processing is in line with the Regulation, both at the time of establishing the means for processing personal data and at the time of their processing (*data protection by design*). Furthermore, according to newly introduced principle of *data protection by default* the controllers would be bound to only process by default those personal data that are necessary for each specific processing purpose, and especially ensure that the data are not collected, stored or disseminated beyond the minimum necessary scope and time in relation to those purposes. It must be ensured that the data are not made accessible by default to indefinite number of people and that data subjects are in the position to control their distribution.[24]

Reporting of a *personal data breach* (accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed) to the supervisory authorities and also to data subjects in certain cases[25], and proper management thereof constitutes a new solution in the draft Regulation. This will in particular be relevant in the cloud computing context and it must as such also be appropriately addressed in joint-controller and controller to processor relationships.

In the overall, emphasis in draft Regulation is placed on controller's strict accountability and responsibility duties. A number of new duties is proposed, such as adoption of policies and implementation of technical and organizational measures so that the controller can ensure and transparently demonstrate compliance of data processing with the Regulation. Also to be mentioned is the duty to have a summary description of these policies and measures in controller's regular general reports, e.g. obligatory reports of publicly traded companies. Furthermore, both the controllers and processors would be bound to maintain regularly updated documentation necessary to fulfill the requirements laid down in the Regulation.[26]

Special attention in draft Regulation is provided to controllers' duties to set up effective internal mechanisms in order to ensure *lifecycle data protection management* (focus on protection of data during their entire lifecycle, *i.e.* as of collection up to erasure or destruction). Both the controllers and processors would be bound to nominate data protection officers in certain cases. Controllers or, where applicable processors, would in certain cases be obliged to carry out risk analyses as to potential impact of intended processing to data subjects' rights and freedoms. A new duty to implement the so-called *data protection impact assessments* is introduced in draft Regulation so as to ensure timely awareness of all possible consequences of data processing operations. Consultations with the data protection officer or with the supervisory authority if the officer was not appointed are proposed steps to be carried out before beginning of relevant data processing (*prior consultation*), in order to mitigate risks where e.g. impact assessment pointed to high risk of processing for data subjects' relevant rights and freedoms.[27]

Regulation also envisages *extensive information duties on processing* to data subjects. This also includes the duty to publish standardized information policies on data processing, which must be clearly visible and easy to understand for data subjects (presented in icons).[28] One of the mandatory information requirements includes information on cases where the data would be transferred outside of the EU. In these cases data subjects must also be informed on existence or absence of the Commission's decision on adequate level of data protection in the country where the data would be exported (as one of the basic conditions when such transfers would be allowed). In other cases, e.g. where transfers are based on *data protection safeguards* (binding corporate rules, European Data Protection Seal, standard data protection clauses adopted by the supervisory authority in accordance with a special procedure and where the Commission declared their general validity, contractual clauses between the controller and processor approved by the supervisory authority), there must be a reference to such safeguards and the means for data subjects to receive their copy.[29]

Alongside the obligation to inform data subjects on details relating to data processing, controllers would also be obliged to respect data subjects' rights, such as a right to request access to their data (which includes a right to various details on their processing), right to correct, erase or block processing of their data in certain cases. We note in particular the newly introduced duty in cases where the data subject files the request electronically and does not ask otherwise, as then the controller should provide requested information electronically, in a structured format. Where possible, in relation to data subjects' requests that are processed automatically, controllers would be bound to ensure that these can be submitted electronically, as well as to ensure that data subjects can

[24] For more details see Article 23 of current draft text.
[25] For more details see Article 4 paragraph 9 and Articles 31-32 of current draft text.
[26] For more details see Articles 22 and 28 of current draft text.
[27] For more details see Chapter IV, section 3 of current draft text.
[28] For more details see Articles 11, 13a (and Annex) and Article 14 of current draft text.
[29] For more details on international transfers, see Articles 40-45a of current draft text.

directly access their data by remote access. In addition to their right to request a copy of their electronically processed personal data in a commonly used electronic and interoperable format, data subjects would also be able to request (where this is technically possible and available) that the controllers, e.g. different service providers, transfer their personal data directly between each other (*data portability principle*).[30]

In the end of this analysis we will briefly point to the fact that tasks and authorities of data protection supervisory bodies, which are specified in detail in draft Regulation, are intended to be harmonized EU-wide. Furthermore, their powers would strengthen significantly. One strong indicator of this is their direct sanctioning authority. Namely, in certain cases they could impose monetary fines amounting to up to 100 000 000 EUR or up to 5 % of annual worldwide turnover (enterprise), depending on which of the two amounts is higher.

V. CONCLUDING REMARKS

Although it is today still unclear if the new EU framework would finally be passed as a regulation that would apply directly in all Member States (or even what its final solutions would entail), fact is that the Commission urges in its Cloud Computing Strategy quick adoption thereof in form of a regulation, so that current diversity of national solutions and legal uncertainty on many cloud computing data protection issues could be resolved as soon as possible. While it may be that the new framework would not provide clear answers to all questions specific for the cloud data processing environment, there is very strong support in it for adoption of sector-specific codes of conduct as voluntary supporting instruments to that effect (previously we noted ongoing development on adoption of the code on the basis of the current framework). Furthermore, draft Regulation envisages powers of the European Data Protection Board, which is to replace the Art. 29 WP, to issue recommendations, guidance and best practices that could address some of the pressing issues. Finally, the Commission itself would be empowered to adopt delegated acts in certain areas, which might also apply to the cloud.

In Croatia, which implemented the General Data Protection Directive in its Personal Data Protection Act, guidance on data protection and cloud computing issued by the Data Protection Agency should be promoted among all stakeholders as well as the general public. Relevant developments at EU legal-regulatory level need to be closely followed so as to already now consider their impact, e.g. controllers' strict accountability and many new duties as analyzed in this paper, as well as duties that would in the future apply also to processors, including their newly introduced direct liability toward data subjects. This would also allow for timely assessment of adjustments, where necessary, to data protection practices and contractual agreements (provider to client, provider to subcontractors). It is important to also consider cloud models that may call for different allocation of roles and responsibilities than that which is characteristic for traditional outsourcing of data processing (provider as processor, client as controller), such as in particular those models where providers' co-controllership over data processing is more realistic. Awareness of available legal mechanisms for data transfers outside the EU is crucial as well as regular keeping track of relevant EU developments, in particular as to use of binding corporate rules and standard contractual clauses in the cloud computing context. It goes without saying that all this should entail regular consultations of guidance and recommendations issued on the topic of data protection and cloud computing, such as in particular those issued by the Art. 29 WP and European Data Protection Supervisor. This is all the more pertinent given that the Art. 29 WP is composed in addition to the European Data Protection Supervisor and Commission's representative, also of representatives of Member States' data protection authorities and thus also the Croatian Agency, which actively participates in its activities. Ideally, all this information should be transparent and easily accessible for the Croatian public, e.g. on Agency's Internet pages (preferably those dedicated to the cloud computing topic). This should also apply to regular updates on important other news in the area, such as the recent positive review of Microsoft's terms for enterprise cloud services with respect to international data transfers. In our opinion all these steps would significantly contribute to the much needed awareness on the subject of data protection and cloud computing, and help clients and providers in Croatia to appropriately address their concerns and assess relevant practices. It has become more and more clear that ensuring and promoting appropriate privacy and data protection practices in the global cloud computing market presents a competitive advantage between various providers. Optimally, providers should consider (further) enhancing transparency on their service Internet pages by clarifying privacy and security practices and terms of their service, thereby also promoting their added value toward potential clients [24].

[30] For more information on data subjects' rights, see especially Articles 10-21 of current draft text.

VI. ACKNOWLEDGMENTS

Research in this paper was supported by the project „Looking to the Future“, which is funded by the Croatian Post and Electronic Communications Agency.

REFERENCES

[1] National Institute of Standards and Technology, “NIST Special Publication 800-145 - The NIST Definition of Cloud Computing”, September 2011, available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[2] “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe”, Brussels, 27.9.2012, COM(2012) 529 final.

[3] ENISA, “Cloud computing - benefits, risks and risk assessment for information security”, 20.11. 2009; “Cloud computing - information assurance framework”, 20.11.2009, “Security & resilience in Governmental clouds – making an informed decision”, 17.11.2011, “Procure secure: a guide to monitoring of security service levels in cloud contracts”, 02.04.2012, “Auditing security measures -an overview of schemes for auditing security measures”, 03.10.2013, “Good practice guide for securely deploying Governmental clouds”, 15.11.2013, “Certification in the EU Cloud Strategy”, 12.11.2013, “Cloud security incident reporting - framework for reporting about major cloud security incidents”, 09.12.2013. All available at: http://www.enisa.europa.eu/.

[4] “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

processing of personal data and on the free movement of such data", Official Journal of the European Union L 281, 23. 11. 1995, pp. 31–50.

[5] 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, 2012/0011 (COD), Brussels, 25.1.2012.

[6] Article 29 Data Protection Working Party, "Opinion 05/2012 on cloud computing", 01037/12/EN, WP 196, 01.7.2012.

[7] I. Lovrek, T. Lovrić, D. Lučić, „Regulatory aspects of cloud computing", Proceedings SoftCOM 2012 International Conference on Software, Telecommunications and Computer Networks, Workshop on Regulatory Challenges, Split, Croatia, 2012; N. Gumzej," Protection of Data Relating to EU Consumers in the IoT Age", Proceedings SoftCOM 2012 International Conference on Software, Telecommunications and Computer Networks, Workshop on Regulatory Challenges, Split, Croatia, 2012; N. Gumzej, "Selected Legal Aspects of Cloud Computing Services", Conference Proceedings CASE 24 – Development of Business and Information Systems, Zagreb, Croatia, 2012.

[8] W. K. Hon, E. Kosta, C. Millard, D. Stefanatou, "Cloud accountability: the likely impact of the proposed EU Data Protection Regulation", Queen Mary School of Law Legal Studies Research Paper No. 172/2014; Tilburg Law School Research Paper No. 07/2014, available at SSRN: http://ssrn.com/abstract=2405971, esp. at pp. 18-19 ; W. K. Hon, C. Millard, I. Walden, "Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing", Part 2 (21.3.2011), International Data Privacy Law, 2012, Vol. 2, No. 1, pp. 3-18; Queen Mary School of Law Legal Studies Research Paper No. 77/2011, available at SSRN: http://ssrn.com/abstract=1794130.

[9] C. Gayrel, J. Gérard, J.-P. Moiny, Y. Poullet, J.-M. Van Gyseghem, "Cloud computing and its implications on data protection", discussion paper for Council of Europe Project on Cybercrime, Namur, Belgium, 05.3.2010, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_ reps_IF10_yvespoullet1b.pdf, at pp. 11-12, 14-16, 21, 26-28; Y. Poullet, J.-M. Van Gyseghem, J.-P. Moiny, J. Gérard, C. Gayrel, "Data protection in the clouds", in Computers, Privacy and Data Protection: an Element of Choice, S. Gutwirth, Y. Poullet, P. De Hert, R. Leenes, Eds., pp. 377-409 at pp. 385-387, 389-391, 406-407.

[10] W. K. Hon, E. Kosta, C. Millard, D. Stefanatou, "Cloud accountability: the likely impact of the proposed EU Data Protection Regulation", Queen Mary School of Law Legal Studies Research Paper No. 172/2014; Tilburg Law School Research Paper No. 07/2014, available at SSRN: http://ssrn.com/abstract=2405971, esp. at pp. 15-21; P. De Hert, V. Papakonstantinou, "The proposed data protection regulation replacing Directive 95/46/EC: a sound system for the protection of individuals", Computer Law & Security Review, vol. 28, issue 2, 2012, pp.130 – 142 at pp. 133-134; I. S. Nwankwo, "Missing links in the proposed EU Data Protection Regulation and cloud computing scenarios: a brief overview," Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 5, issue 1, 2014, pp. 32-38 at pp. 35-36, available at: https://www.jipitec.eu/issues/jipitec-5-1-2014/3905/jipitec_5_1_ nwanko.pdf.

[11] European Commission, "Commission decisions on the adequacy of the protection of personal data in third countries", available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-14.

[12] European Commission, "Model contracts for the transfer of personal data to third countries", available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

[13] European Commission, "Overview on binding corporate rules", available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

[14] European Commission, "Commission decisions on the adequacy of the protection of personal data in third countries – US - United States - Safe Harbor", available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/ adequacy/index_en.htm# h2-14.

[15] European Commission, "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", Official Journal of the European Union L 39, 12.2.2010, pp. 5-18.

[16] Article 29 Data Protection Working Party, "Letter to Microsoft, Ref. Ares(2014)1033670 - 02/04/2014", Brussels, 02.4.2014, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document /files/2014/20140402_microsoft.pdf.

[17] Official Gazette of the Republic of Croatia nos. 103/03, 118/06, 41/08 and 130/11 – consolidated text published in no. 106/12.

[18] Official Gazette of the Republic of Croatia no. 139/04, Article 8 of the Personal Data Protection Act.

[19] Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, "Orientierungshilfe – Cloud Computing", 26.9.2011, available at: http://www.bfdi.bund.de/DE/Themen/TechnologischerDatenschutz/TechnologischeOrientierungshilfen/Artikel/OHCloudComputing.pdf?__blob=publicationFile; Information Commissioner, "Personal data protection & cloud computing", 15.6.2012, available at: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf; Datainspektionen, "Cloud services and the Personal Data Act", available at: http://www.datainspektionen.se/Documents/faktablad-cloudservices.pdf; Úřad pro ochranu osobních údajů, "K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb", 27.8.2013, available at: http://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002; Il Garante per la protezione dei dati personali, "Cloud computing - how to protect your data without falling from a cloud", available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906139; Agencia Española de Protección de Datos, "Guía para clientes que contraten servicios de cloud computing", 2013, available at: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf; "Orientaciones para prestadores de servicios de cloud computing", 2013, http://www.agpd.es/portalwebagpd/canaldocumentacion/publicaciones/common/guias/orientaciones_cloud.pdf; Information Commissioner's Office, "Guidance on the use of cloud computing", 2012, available at: http://ico.org.uk/for_organisations/data_protection/topic_guides/online/cloud_computing; La Commission Nationale de l'Informatique et des Libertés, "Cloud computing: les conseils de la CNIL pour les entreprises qui utilisent ces nouveaux services", 25.6.2012, available at: http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-les-conseils-de-la-cnil-pour-les-entreprises-qui-utilisent-ces-nouveaux-services/.

[20] S. Grgić, Personal Data Protection Agency, "ISO 27001 personal data protection and cloud computing" (original title: "ISO 27001 zaštita osobnih podataka i računalstvo u oblaku"), 2012.

[21] "Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"", Brussels, 16.11. 2012, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/ Consultation/Opinions/2012/12-11-16_Cloud_ Computing_EN.pdf , esp. at pp. 13-14.

[22] P. De Hert, V. Papakonstantinou, "The proposed data protection regulation replacing Directive 95/46/EC: a sound system for the protection of individuals", Computer Law & Security Review, vol. 28, issue 2, 2012, pp.130 – 142 at p. 134.

[23] European Commission, Digital Agenda for Europe, Telecoms and the Internet, Cloud Computing, European Strategy, Working Groups, "The Cloud Select Industry Group on Code of Conduct", available at: https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct; European Commission, Press releases, "New guidelines to help EU businesses use the Cloud", IP/14/743, Brussels, 26.6.2014, available at: http://europa.eu/rapid/press-release_IP-14-743_en.htm.

[24] One example of a company succesfully practising such approach is Microsoft, see e.g.: http://office.microsoft.com/hr-hr/business/centar-za-pouzdanost-sustava-office-365-sigurnost-servisa-u-oblaku-FX103030390.aspx (pages intended for the Croatian market); http://blogs.technet.com/b/microsoft_blog/archive/2014/04/10/privacy-authorities-across-europe-approve-microsoft-s-cloud-commitments.aspx.