27 June 2013

Croatia set to join the European Union: What this means for data protection compliance

By Karin Retzer and Alja Poler De Zwart

On July 1, 2013, the Republic of Croatia will become the twenty-eighth Member State of the European Union (EU)[1]. Croatia's accession is the result of ten years of rigorous efforts, which started with its application for membership in 2003. Originally, Croatia had been aiming for a 2007 accession date. The negotiations, however, turned out to be more difficult than expected and, most notably, were prolonged for ten months by unresolved and long-running border and banking disputes[2] with its northern neighbor, the EU Member State of Slovenia.

The current EU Member States ultimately signed Croatia's Accession Treaty[3] in December 2011. A referendum on EU accession was held in Croatia on January 22, 2012, with 66.27% of participants voting in favor of Croatia joining the EU. After a lengthy monitoring process, the European Commission (the "Commission") confirmed in its final Monitoring Report on Croatia's accession preparations issued on March 26, 2013[4] that Croatia has completed the ten priority actions identified in the Commission's previous Comprehensive Monitoring Report.[5] These actions include commitments in the area of competition, and the judiciary and fundamental rights of justice, freedom and security. At the same time, Croatia is generally meeting the conditions and requirements arising from the accession negotiations in all 35 acquis chapters. The Commission also noted that it was confident that the country will be ready for EU membership on July 1, 2013

[1] The 27 Member States of the European Union currently are: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom (collectively, the "Member States").

[2] In respect of the border dispute, both parties finally agreed to international arbitration. In respect of the banking dispute, the parties settled for the time being.

[3] Council of the European Union Accession Treaty concerning the accession of the Republic of Croatia 14409/11, November 7, 2011.

[4] COM(2013) 171 final, Communication From the Commission to the European Parliament and the Council of March 26, 2013.

[5] COM(2012) 601 final, Communication From the Commission to the European Parliament and the Council on the Main Findings of the Comprehensive Monitoring Report on Croatia's State of Preparedness for EU Membership of October 10, 2012.

UNITED STATES

California

Tiffany Cheung	(415) 268-6848
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
James R. McGuire	(415) 268-7013
Daniel F. Muto	(858) 720-7959
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
David M. Walsh	(213) 892-5262

New York

Cindy Abramson	(212) 336-4178
Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Sherman W. Kahn	(212) 468-8023
Mark P. Ladner	(212) 468-8035
Peter McLaughlin	(212) 336-4290
Michael B. Miller	(212) 468-8009
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213

Washington, D.C.

Nicholas A. Datlowe	(202) 887-1590
L. Richard Fischer	(202) 887-1566
D. Reed Freeman, Jr.	(202) 887-6948
Julie O'Neill	(202) 887-8764
Obrea O. Poindexter	(202) 887-8741
Cynthia J. Rich	(202) 778-1652
Andrew M. Smith	(202) 887-1558
Nathan David Taylor	(202) 778-1644

EUROPE

Brussels

Joanna Łopatowska	32 2 340 7365
Karin Retzer	32 2 340 7364
Alja Poler De Zwart	32 2 340 7360

London

Ann Bevitt	44 20 7920 4041
Anthony Nagle	44 20 7920 4029
Caroline Stakim	44 20 7920 4055
David Varney	44 20 7920 4058

ASIA

Beijing

Gabriel Bloch	86 10 5909 3367
Jingxiao Fang	86 10 5909 3382
Paul D. McKenzie	86 10 5909 3366

Hong Kong

Gordon A. Milner	852 2585 0808

Tokyo

Daniel P. Levison	81 3 3214 6717
Gabriel E. Meister	81 3 3214 6748
Jay Ponazecki	81 3 3214 6562
Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

and that the "*EU membership is an additional incentive to continue reforms in Croatia. Building on the achievements to-date, Croatia is expected to continue developing its track record in the field of the rule of law, notably in the fight against corruption*."

As an EU Member State, Croatia shall also be required to:

- join the Schengen Area, a group of twenty-six European countries which allow free movement of persons, effectively abolishing national borders in favor of a single, external border. According to several media reports, Croatia wishes to enter the Schengen Area by 2015, but it remains questionable whether it will fulfill all of the necessary criteria by then;
- qualify for the free movement of workers across the EU by implementing rules on the free movement of workers in the Schengen Area that will be phased in over a transition period, currently expected to be approximately two years; and
- adopt the common market currency, the Euro accession to the Eurozone which is a separate process presided over by the European Central Bank and the Commission's Directorate-General for Economic and Financial Affairs and fulfill a number of criteria and demonstrate economic stability in order to join the Eurozone. It may be several years before this happens.

DATA PROTECTION IMPLICATIONS

Below we set out the main particularities of the Croatian data protection framework that may have an impact on and may need to be observed by multinational businesses operating in Croatia.

Legal Framework: According to the information provided on the website of the Croatian Personal Data Protection Agency (the "Croatian DPA"), Croatia's Act on Personal Data Protection[6] (the "Croatian Act") dates back to 2003, has been revised several times in recent years and "*has been harmonized in all important questions*"[7] with the EU Data Protection Directive 95/46/EC[8] (the "Directive").

As of July 1, 2013, not only the Directive but also the guidance issued by the consortium of European data protection regulators, the Article 29 Working Party (WP29) will be applicable to organizations established in Croatia.

The European ePrivacy Directive 2002/58/EC (as amended by Directive 2009/136/EC)[9] will also apply to providers of electronic telecommunications services operating in Croatia through the amended Croatian Electronic Communications Act[10] which shall enter into force on the day of accession. The Electronic Communications Act implements the amended ePrivacy Directive that introduced a number of far-reaching obligations of electronic telecommunications service providers (e.g., data security breach notification, direct marketing and use of cookies). The required obligations mean that the providers operating in Croatia, as well as the operators of any website targeting Croatian users will need to update their

[6] Official Gazette No. 103/03, No. 118/06 & No. 41/08.

[7] See http://www.azop.hr/page.aspx?PageID=50.

[8] Directive 95/46/EC of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on free movement of such data [1995] OJ L 281/31.

[9] Directive 2002/58/EC of the European Parliament and of the Council of July 12 concerning the processing of personal data and the protection of privacy in the electronic communications sector of July 12, [2002] OJ L 201/37 amended by Directive 2009/136/EC of the European Parliament and of the Council of November 12, [2009] OJ L 337.

[10] Official Gazette No. 73/08, No. 90/11 & No. 133/12. The official consolidated (Croatian) version is available at http://www.propisi.hr/print.php?id=8239.

privacy and data protection policies and procedures to ensure compliance with the Electronic Communications Act. This implementation is a welcomed and much needed addition to the Croatian data protection framework, since the previous Croatian regulation did not cover the abovementioned topics and data security breach notification requirements for data controllers were non-existent.

Croatia's accession also means that any new EU legislation adopted, in particular the Commission's draft General Data Protection Regulation[11] ("draft Regulation"), will apply to Croatia.

The Regulatory Authority: The Croatian DPA is the responsible regulatory authority in Croatia and will continue to supervise compliance with the Croatian Act. The Croatian DPA has the power to refer cases of non-compliance to the municipal courts and the power to conduct compliance audits, either following a complaint or on its own initiative. Since being elected a candidate country in 2003, Croatia has been an active observer in EU institutions, including the WP29. After the accession, the Croatian DPA will become a full member of the WP29.

Separate Regulatory Body for Freedom of and Access to Information: One of the changes required by the Commission was the creation of a separate regulatory body for freedom of and access to information. On February 15, 2013, Croatia therefore adopted a new Law on Access to Information.[12] This new law introduces the so-called proportionality and public interest test in all cases of denial of access to information and implements the EU acquis on the re-use of information. The most significant novelties of the Law on Access to Information relate, amongst others, to:

- the implementation of Directive 2003/98/EC on the re-use of public sector information;[13]
- the introduction of the Commissioner of Access to Information who will act as an independent authority (appointed by Parliament) and whose main tasks will be to protect the right of access to information and serve as an appellate authority for resolving complaints;
- the obligation for the public sector to publish on the Internet, in an easily searchable and accessible manner, all laws and regulations, drafts of the laws and other regulations, annual plans and enactments and all other relevant information pertaining to its work; and
- the introduction of the central catalogue of official documents of the Republic of Croatia, which shall be provided by the Croatian Information and Documentation Referral Agency (HIDRA).

The Commission's final Monitoring Report on Croatia's accession preparations stipulated that, in the exercise of their respective mandates, the Croatian DPA and the new Commissioner of Access to Information must ensure the coherence of any decisions they make.

[11] Proposal for a Regulation of the European Parliament and of the Council for 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 (January 25, 2012).

[12] Official Gazette No. 25/13 on February 28, 2013.

[13] Directive 2003/98/EC of the European Parliament and the Council of November 17, 2003 on the re-use of public sector information.

Cross-Border Transfers: Croatia's data protection regime was never officially deemed adequate by the Commission. Therefore, for the purposes of personal data transfers from EEA countries[14] to Croatia, it was necessary to have adequate safeguards in place. Since the Directive provides for free movement of personal data within the EEA, cross-border transfer mechanisms for third countries will no longer be required for transfers between the EEA and Croatia. However, companies will still need to conclude appropriate data processing agreements with their service providers.

The Croatian DPA ascribed to the Commission's adequacy findings, but also seems to consider Albania, Bosnia and Herzegovina, and Macedonia as having adequate levels of data protection (see the list of the adequate countries according to the Croatian DPA at http://www.azop.hr/page.aspx?pageID=47). Please note that the Commission has not deemed these countries to be adequate. Any transfer of personal data via Croatia to these non-adequate countries will therefore still need to comply with EU transfer requirements for transfers to non-adequate countries. Transfers of personal data to non-adequate countries require the consent of an individual or an appropriate safeguard such as Standard Contractual Clauses (model contracts adopted by the Commission), ad-hoc contracts, the U.S. Safe Harbor framework, or Binding Corporate Rules (BCRs). Alternatively, the transfer may benefit from one of the exemptions, such as where the transfer is necessary to fulfill a contract with an individual (contractual necessity), or is in the legitimate interest of a data controller (balance of interest). In Croatia, the use of Standard Contractual Clauses, ad-hoc contracts, or the U.S. Safe Harbor framework does not require the Croatian DPA's approval, but contracts must be translated into Croatian (note that an individual's consent is also required where ad-hoc contracts are used). BCRs can be used subject to the Croatian DPA's approval, as well as the approval of the data protection authorities in the other Member States concerned. However, it seems that the Croatian DPA does not yet participate in the mutual recognition procedure,[15] meaning that businesses might not be able to benefit from the streamlined approval process.

Organizations must also ensure that database registrations filed with the Croatian DPA are up to date with information on cross-border transfers. Registrations must indicate whether personal data have been transferred to or from Croatia, the destination third country or foreign recipient, the purpose of the transfer and the legal basis for the transfer.

Data Security: Croatia has very detailed security measures set forth in the Regulation on the Procedure for Storage and Special Measures Relating to the Technical Protection of Special Categories of Personal Data, which dates back to 2004. In particular, the Regulation lays down measures, tools and conditions for the storage, safety, security and transfer of special categories of personal data and the corresponding data filing systems. It also specifies:

- the measures for the maintenance and control of the computer and telecommunications equipment and related software of the system;
- the protective measures to be taken to physically secure the working premises and equipment, and the persons authorized to implement the measures;
- the persons competent to supervise the implementation of the measures; and

[14] The European Economic Area (EEA) comprises the Member States of the European Union, as well as Iceland, Liechtenstein and Norway.

[15] At the moment, 21 EEA countries are part of the mutual recognition procedure: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Estonia, France, Germany, Iceland, Ireland, Italy, Latvia, Liechtenstein, Luxembourg, Malta, the Netherlands, Norway, Slovakia, Slovenia, Spain, and the United Kingdom. Source: http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm.

- additional security provisions for filing systems that contain manually processed special categories of personal data.

Appointment of a Data Protection Officer: Organizations that employ more than 20 employees must appoint a "security officer". If they employ less than 20 employees, a security officer may be appointed, but they are not required to do so.

Sanctions: Administrative fines for non-compliance with the Croatian Act range from HRK 20,000.00 (approx. US$3,500) to HRK 40,000.00 (approx. US$7,000). The fines may be applied to a legal entity and, in some cases, to the person responsible within the legal entity.

The new Electronic Communications Act provides, among other terms, that a legal person may be punished with a fine ranging from HRK100,000.00 (approx. US$17,500) to HRK1 million (approx. US$175,000) if it fails to comply with the provisions of the act pertaining to data security breaches (article 99a), cookies (article 100(4)) and direct marketing (article 107). A responsible person within the legal entity may also be punished for the breaches referred to above with a fine ranging from HRK20,000 to 100,000.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for eleven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law*," or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.