GDPR implementation in Croatian data protection law

Marija Gregorić and **Lovro Klepac** of Babic & Partners Law Firm LLC discuss Croatia's implementation of the GDPR and the scope of application of the national law.

The Croatian Act on Implementation of General Data Protection Regulation (Official gazette no. 42/2018) ("GDPR Implementing Act" or "Act") entered into force on 25 May 2018, following the start of application of the Regulation (EU) 2016/679 (GDPR) across all EU Member States. The GDPR Implementing Act supplements the GDPR and also introduces derogations from its specific rules.

The GDPR Implementing Act expressly excludes from its material scope the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection from threats to public security, as well as the area of national security and defence. Furthermore, the Act does not contain general provisions expressly referring to its territorial or personal scope of application. However, the rules on specific processing operations within the Act expressly define their personal and territorial scope, notably (i) provisions concerning a child's consent in relation to the offer of information society services to a child; (ii) provisions governing the processing of genetic data in the context of entry into and performance of life insurance agreements or endowment clauses; and (iii) provisions governing the processing of biometric data. These provisions are further elaborated below.

SPECIFIC PROCESSING OPERATIONS

The GDPR Implementing Act makes use of the GDPR's opening clauses and introduces additional requirements for a child's consent related to the offer of information society services, processing of genetic and biometric data and the processing of personal data by means of video surveillance.

A child's consent related to an offer of information society services: In relation to the data processing in the context of offering of information society services directly to a child, the Act does not lower the age of child consent below 16 years or impose additional requirements for such data processing. The Act provides that the processing of a child's personal data under Article 6(1)(a) GDPR is lawful if the child is at least 16 years of age. The above applies to any child residing in Croatia. An infringement of the above rules is considered as a violation of Article 8 of the GDPR and is subject to sanctions under Article 83 of the GDPR.

GDPR Derogations applicable to the processing of special categories of personal data: The GDPR Implementing Act has made use of the opening clause contained in Article 9(4) of the GDPR by introducing further conditions with regard to the processing of genetic and biometric data. The Act prohibits the processing of genetic data for the purpose of assessing the data subject's illness or other health aspects relating to the conclusion or performance of life insurance agreement or an agreement with endowment clause.[1] The above prohibition cannot be lifted by the data subject's explicit consent and applies if (i) the data subject enters into the above agreement in Croatia and (ii) the data is processed by the data controller established in Croatia or providing services in Croatia.[2]

The Act sets out rules on processing of biometric data in the private and public sectors. Entities in the public sector may process biometric data only if the following conditions are cumulatively met: (i) applicable law requires the processing, (ii) the data subject's interests do not override the interests of the processing, and (iii) the processing is necessary for the protection of individuals, assets, classified information or business secrets.[3] The lawfulness of biometric data processing is presumed where such processing is necessary for performance of treaty obligations related to the identification of individuals at state border crossings.[4]

Entities in the private sector are allowed to process biometric data only if either (i) such processing is mandated under the law, or (ii) processing is necessary for protection of persons, assets, classified information, business secrets or for individual and secure identification of users, provided that there are no overriding interests of data subjects contrary to the processing. Under Article 22(2) of the Act, the legal basis for processing of biometric data for individuals and secure identification of users is the data subject's (i.e. user's) explicit consent.

Article 23 of the Act expressly allows the processing of employees' biometric data for the purpose of recording working hours and for the purpose of workplace access control, if either (i) such processing of employees' biometric data is mandated under the law or (ii) such processing is performed as an alternative to another technical solution for recording of working hours or access control, provided that the employee has given his/her explicit consent to processing.

In general, under Article 24 of the GDPR Implementing Act, the rules on processing of biometric data apply to data subjects in Croatia if the processing is conducted by either a data controller established/providing services in Croatia or a public authority.

Data processing by means of video surveillance: The GDPR Implementing Act has introduced detailed rules on (i) video surveillance in general, (ii) video surveillance of work premises, (iii) video surveillance of public areas, and (iv) video surveillance of residential buildings. Croatia's Personal Data Protection Agency (DPA) has recently issued an opinion clarifying which types of video surveillance are caught by the application of GDPR and the Act.[5] According to the above opinion and Article 25 of the Act, the GDPR and the Act only apply to video surveillance that utilizes a filing system for storage of personal data. In this regard, if the personal data is processed by a livestream (e.g. web camera) which does not have a filing system, such processing is outside the

scope of GDPR and the Act.[6]

Under Article 26 of the GDPR Implementing Act, video surveillance is allowed only if necessary and justified for protection of persons and assets, provided that the data subject's interests do not override the interests of processing. Furthermore, the video surveillance perimeter must be limited to interior premises (and/or parts thereof), the exterior surface of the building or structure, or the interior of public transportation vehicles. Article 27 of the Act provides for the obligation of the controller or processor to provide the data subjects with information contained in Article 13 of the GDPR and to post a clear and easily understandable sign visible when entering the recording perimeter which indicates: (i) the premises/area is under video surveillance, (ii) information on the data controller, and (iii) contact details for exercising data subject rights.

Video surveillance data may be accessed exclusively by the responsible individual/manager of the data controller or processor, or the person authorized by such individual, and by competent authorities within performance of their duties.[7] Under Article 29 of the GDPR Implementing Act, video surveillance recordings may be retained for a maximum of six months, unless a special law requires a longer retention period, or if such recordings are used as evidence in judicial, administrative, arbitration or other equivalent proceedings. The Act introduces additional requirements applying to video surveillance of work premises, residential buildings and public areas.

Data processing for statistical purposes: Under Article 33 of the Act, certain data subjects' rights guaranteed under the GDPR do not apply in relation to the processing of personal data for official statistical purposes. The competent statistics authorities are not required to ensure the right of access, right of rectification, right to restriction of processing or the right to object to processing by data subjects. The above limitations on data subjects' rights only apply where necessary for achieving the official statistics purposes and only to the extent the exercise of data subjects' rights would impede or seriously endanger such purposes. Furthermore, data controllers are not required to inform the data subjects in accordance with Articles 13 and 14 of the GDPR when sharing personal data with the statistics authorities.

The Act allows for secondary processing for statistical purposes and provides that the processing of personal data for statistical purposes shall be considered compatible with the original purpose for which data was collected, subject to implementation of appropriate safeguards for protection of personal data. Under Article 33(5) of the Act, data processed for statistical purposes shall not allow identification of a data subject.

Supervisory authority

The supervisory authority competent for performance of tasks and exercise of powers conferred to it in accordance with the GDPR is the Croatian Personal Data Protection Agency (DPA). The Act confers certain additional powers to the DPA, other than those expressly provided under Article 58 of the GDPR, including the DPA's right to initiate and participate in criminal, administrative and other proceedings for violations of GDPR and the Act when authorized by a special law.[8] The Act introduces procedural rules governing data protection audits conducted by the DPA under Article 58(1)(b) of the GDPR. The data protection audit may be conducted either (i) as an audit based on a prior notice to the controller/processor or (ii) as a dawn-raid, in both cases based on an order issued by the DPA's director.[9]

Administrative fines

The DPA may issue administrative fines for violations of the GDPR and the GDPR Implementing Act. The GDPR Implementing Act contains two categories of rules on administrative fines for violations of the Act.

First, the Act expressly provides that infringements of certain of its provisions constitute violations of GDPR. For example, the Act provides that a violation of rules governing the minimum age of consent in relation to offer of information society services constitutes an infringement of Article 8 of the GDPR and is subject to sanctions in accordance with Article 83 of the GDPR. Furthermore, Article 20(4) of the Act provides that a violation of the Act's provisions on genetic data processing constitutes an infringement of Article 9 of the GDPR and is subject to sanctions in accordance with Article 83(5) of the GDPR.

Second, Article 51 of the Act sets out the administrative fine of 50,000 Croatian kuna (approximately €6,800) for a violation of the duty to inform data subjects about video surveillance, violation of the duty to establish an automated system for recording access to video surveillance recordings and for the use of video surveillance data contrary to the purpose of video surveillance processing defined in the Act.

The GDPR Implementing Act has made use of the opening clause contained in Article 83(7) of the GDPR, which allows EU Member States to lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. Under Article 47 of the Act, Croatian public authorities are exempt from administrative fines for violations of GDPR and/or GDPR Implementing Act.

AUTHORS

Marija Gregorić is a Partner, and Lovro Klepac an Associate at Babic & Partners Law Firm LLC, Zagreb, Croatia.
Emails: Marija.Gregoric@babic-partners.hr
Lovro.klepak@babic-partners.hr

REFERENCES

1 Article 20(1) of the GDPR Implementing Act (available at: narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html).
2 Articles 20(2) and 20(3) of the GDPR Implementing Act (available at: narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html).
3 Article 21 of the GDPR Implementing Act (available at: narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html).
4 *Ibid*.
5 Opinion of Croatian Data Protection Authority on Video surveillance – livestreaming dated 7 June 2019; available at: azop.hr/misljenja-agencije/detaljnije/videonazdor-livestreaming
6 *Ibid.*
7 Article 28(1) of the GDPR Implementing Act (available at: narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html).
8 Article 6(1) of the GDPR Implementing Act (available at: narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html).
9 Article 36 of the GDPR Implementing Act (available at: narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html).

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Belgium's DPA aims at mediation rather than fines

Previously the DPO for Nielsen, the new Belgian DPA brings both academic insight and a business experience to his regulatory role. **Stewart Dresner** and **Laura Linkomies** report.

Dr David Stevens was appointed as Chairman of Belgium's DP Authority on 28 March 2019, together with the other members of the Executive Committee of the Belgian Data Protection Authority. The delay in appointments was partly due to strict language requirements; the GDPR implementing Act was adopted in 2018 and entered into force on 5 September 2018 (*PL&B International* February 2019, p.1).

Dr Stevens is an experienced data

Continued on p.3

National approaches to 'legitimate interest' trouble EU

The European Commission's unease over national implementation of the GDPR also encompasses limits to data subjects' rights and 'effective' independence of DPAs. **Tom Cooper** reports.

The European Commission is continuing bi-lateral and group discussions with Member States as it pursues the harmonisation of data protection rules across the bloc. But multi-state operators remain wary of tripping over national variations in the implementation of the EU General Data Protection Regulation (GDPR). Karolina Mojzesowicz, Deputy Head, Data Protection Unit, European Commission, confronted

Continued on p.4

Issue 160 **AUGUST 2019**

INTERNATIONAL report

ISSUE NO 160 AUGUST 2019

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Robert Waixel
Anglia Ruskin University, UK
Laura Drechsler
Brussels Privacy Hub, Belgium
Marija Gregorić and Lovro Klepac
Klepac, Babic & Partners LLC, Croatia
Katrine Plavina
Vilgerts, Latvia
Wenlong Li
University of Edinburgh, UK
Frank Madden
IBM, UK
Will Stern and Sabrina McGraw
Covington & Burling LLP, US
Dino Wilkinson
Clyde & Co, United Arab Emirates

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Data protection is taken seriously – also in the US

The $5 billion fine imposed on Facebook by the US Federal Trade Commission is the largest we have seen for a privacy violation (p.32) and will perhaps influence EU DPAs in their enforcement. However, a ban on certain types of processing may be more effective than any fine when talking about a company the size of Facebook. Europe has yet to see such a large GDPR fine. *PL&B's* interview with Belgium's new Data Protection Commissioner reveals that he in fact regards mediation as more effective than fines (p.1).

On Internet giants and surveillance capitalism, read Graham Greenleaf's analysis of Shoshana Zuboff's thought-provoking book on p.29.

The European Commission monitors the Member States' implementation of the GDPR, and much work still remains to be done. In some instances, Member States have introduced national requirements on top of the Regulation, in particular, through many sectoral laws. This practice leads to fragmentation and results in creating unnecessary burdens, the Commission says in its recent Communication . Speaking at our Annual Conference in Cambridge in July, Karolina Mojzesowicz, Deputy Head, Data Protection Unit, European Commission, said that the Commission has taken a "very proactive" approach to the implementation of the Regulation, working with Member States to discuss options, possibilities and solutions. It continues to analyse national legislation and to clarify issues in bilateral discussions (p.1).

We follow closely the Commission's work in this field which will result in a report in 2020 (p.10). In this issue, we are pleased to bring you news from two more countries in our series of articles on GDPR implementation at national level; our correspondents from Latvia (p.16) and Croatia (p.14) discuss their countries' laws, which have both been in force since last summer.

Another area of work at the EU Commission is to review the existing adequacy decisions and evaluate any new national applications for an adequacy assessment. With Japan having achieved the mutual adequacy decision, Korea is next in line (p.6). The G20 is discussing an overarching framework that promotes cross-border data flows (p.18), and the next EU-US Privacy Shield review will begin in mid-September.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 125+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 125+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**"

Subscription Fees

Single User Access

International Reports **£560 + VAT***
UK Reports **£450 + VAT***
UK & International Reports **£900 + VAT***
* VAT only applies to UK based subscribers

Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions
Rest of Europe = £50, Outside Europe = £70

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK