

Data Privacy Alert

16 November 2016

In this issue:

The Ministry of Health published a Project Norms for the implementation of the Law on patients' rights no. 46/2003

Sanctions imposed by the Data Protection Authority

Notifications of Yahoo and WhatsApp by the Article 29 Working Party

Statement of the Working Party 29 on the EU – US Umbrella Agreement



The Ministry of Health published a Project Norms for the implementation of the Law on patients' rights no. 46/2003

On October 21, the Ministry of Health published on its website the Project Norms for the implementation of the Law on patients' rights no. 46/2003 (the "Norms"). The Norms are intended to provide a procedure through which the patients may exercise their rights under Law of patients' rights no. 46/2003, including with respect to the access to their personal data, such as:

- *The obligation to obtain the express consent of the patient in case the patient is to be photographed/filmed*
If the patients are filmed or photographed in the healthcare facilities, their prior express consent must be obtained.
There are two exceptions from this rule, namely when the images thus obtained are necessary (i) for determining the diagnosis/treatment of the patient or (ii) the avoidance of suspicions regarding malpractice.
- *The healthcare facilities must assure the unlimited access of patients to their personal medical data*
- *The use of personal data regarding the family and personal life of the patient*
If the personal data regarding the private and family life of the patient influence in a positive manner the diagnosis process or treatment, the healthcare facilities may use such data. However, such personal may be used only with the express consent of the patient.
The Norms also provide two exceptions from this rule: (i) the case where the patient represents a danger to himself or (ii) if the patient represents a threat to public safety.
- *The patient may grant access to his personal medical data to another person*
The patient has the right to choose to not to be informed in the case the respective medical information may cause him grief.

Furthermore, the patient has the right to choose another person to receive the respective information in his place. The patient may grant access to his medical personal data in writing. Such access may be withdrawn at any time by the patient also through a written notice.

Sanctions imposed by the Data Protection Authority

According to the information available on the official website of the Romanian Data Protection Authority (the "DPA"), in September - October 2016, the DPA carried out several inspections ex officio or following the complaints or notices received and applied administrative fines.

As effect of these inspections, several banks and companies providing financial services have been sanctioned for illegal processing of personal data. The illegal processing of personal data consisted, amongst others, in:

- Submission of negative data to Biroul de Credit SA for several natural persons without proving the prior information of the data subject; and
- Submitting several times during the same month negative data to Biroul de Credit SA for the same delay of payment (taking into account the obligation of payment due). Submission of these negative data does not observe the 30 days deadline which breaches the provisions of Decision no. 105/2007 on the processing of personal data in credit bureau type evidence systems, corroborated with the provisions of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

The maximum fine imposed by the DPA is of 25,000 lei.

Notifications of Yahoo and WhatsApp by the Article 29 Working Party

On October 27, 2016, the Article 29 Working Party (the "WP29") addressed a letter to WhatsApp regarding the update of its Terms of Service and Privacy Policy announced last August and a letter to Yahoo regarding the data breach occurred in 2014 and, respectively, the scanning of customer emails for intelligence purposes.

According to the WP29 press release, both the WhatsApp Terms of Service and Privacy Policy Update and the Yahoo data breach and scanning of user emails, will be discussed at the first meeting of the WP29 enforcement subgroup, in November.

Regarding WhatsApp updated Terms of Service and Privacy Policy, WP29 raised concerns regarding the sharing of information within the "*Facebook family of companies*" for purposes that were not mentioned in the Terms of Service and Privacy Policy, as well as regarding the validity of the user's consent regarding such a policy change.

In the letter addressed to Yahoo, WP29 requested information and clarifications regarding:

- The admitted 2014 data breach, whereby personal data related to at least 500 million Yahoo.Inc users were stolen;
- The alleged scanning of Yahoo's customer incoming emails for US intelligence purposes at the request of US intelligence agencies.

Statement of the Working Party 29 on the EU – US Umbrella Agreement

On October 26, 2016, the Working Party 29 (the “**WP29**”) issued a statement regarding the “Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences” (“**Umbrella Agreement**”).

The Umbrella Agreement was signed on June 2, 2016, but has not yet become effective.

According to the statement, WP29 welcomes the initiative to set up a general data protection framework for EU-US law enforcement cooperation. However, WP29 mentions that certain clarifications may be needed in order to ensure a level of protection under the Umbrella Agreement, which is consistent with the level of protection offered by EU law.

The main point highlighted by WP29 as requiring further attention are:

- the definitions of the concepts of “personal data” and “data processing” differ from the EU definitions;
- the data retention period should be defined more strictly in relation to the purpose pursued;
- the restrictions to individual’s access rights are very broad and access could be improved by the establishment of an indirect access right mechanism.

For further questions regarding the aspects mentioned in this alert, please contact us.

Andrei Burz-Pînzaru

Partner Reff & Associates
+40 21 2075 205
aburzpinzaru@reff-associates.ro

Andrei Ionescu

Partner Risk Advisory Deloitte
+40 21 2075 485
aionescu@deloittece.com

Cătălin Țigănilă

Director Risk Advisory Deloitte
+40 21 2075 280
ctiganila@deloittece.com

Silvia Axinescu

Managing Associate Reff & Associates
+40 730 585 837
maxinescu@reff-associates.ro



This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, any of its member firms or any of the foregoing's affiliates (collectively the "Deloitte Network") are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/ro/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Reff & Associates SCA is a law firm member of Bucharest Bar, independent in accordance with the Bar rules and represents Deloitte Legal in Romania. Deloitte Legal means the legal practices of Deloitte Touche Tohmatsu Limited member firms or their affiliates that provide legal services. Visit the global Deloitte Legal website <http://www.deloitte.com/deloittelegal> to see which services Deloitte Legal offers in a particular country.

The efficient management of the issues pertaining to personal data legal framework requires a multidisciplinary approach, addressing both purely legal matters, but also their correlation with operational and risks management aspects. In this respect, combined teams including lawyers within Reff & Associates, as well as specialists from Risk Advisory department within Deloitte, address all aspects pertaining to the process regarding the management of compliance with personal data regulations, using both local know how, as well as applicable best practices in this field.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 225,000 professionals are committed to making an impact that matters.