WHY OPERATORS NEED TO BE AWARE OF THE NEW DATA PROTECTION RULES

Posted by: Andrew McCarron April 25, 2017 in Betting on Football, Featured News, Interviews, Latest News
Comments Off

Professor Alessandro del Ninno, an advocate at Italian law firm **Tonucci & Partners**, will be presenting an update on the incoming rules over data protection that operators have to be mindful of at next week's **Betting on Football Conference**. SBC caught up with him ahead of the show to discuss why it is so important.

SBC: The EU General Data Protection Regulation is set to be enacted in May 2018. Why do operators need to be wary of this?

Alessandro del Ninno: The EU General Data Protection Regulation – enacted on April 27, 2016 – shall be applicable starting from May 25th, 2018. Companies should start since now the review process of their data processing policies and privacy organization, since the fulfilments to be implemented (from a technical, organisational, documental and security perspectives) are of a major importance and need time to be carefully implemented.

It is also important to point out that the GDPR is not only a European "law": even not EU-based entities must entirely comply if the processing of personal data of data subjects who are in the Union relates to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. So, if we look – for example – at the betting services offered to EU users and at the companies' interest into profiling/monitoring, the consequence is that the pre-requirements above make the GDPR applicable to world betting operators – even not EU based – offering the services in the EU.

In another different perspective, I further think that operators should be interested in fully complying with the GDPR also as a commercial strategy: increasing the customers' awareness of a provider protecting and lawfully processing his/her personal data for sure is a way to foster customers' loyalty.

FEATURES


Why operators need to be aware of the new data protection rules
April 25, 2017


Matt Wilson: Ball Street – No Hype… Why Fan Media should matter to all industry stakeholders
April 24, 2017


Darren Moore – Betting Gods – Connecting with major partners in Malta
April 21, 2017


Susan O'Leary – Alderney – Strength in numbers
April 19, 2017


Jonathan Patterson – Qubit – Key Discipline…why personalisation marks the difference…
April 18, 2017

SBC: What effect will the GDPR have on how companies profile their customers?

AdN: In the GDPR profiling is considered one of the most sensitive data processing. For the first time we have in a data protection law even the definition of "profiling": "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

From a practical point of view, I may briefly summarise what fulfillments are required to be complied with by operators profiling their customers:

- (a) a specific prior procedure called "data protection impact assessment" (PIA) must be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment must include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with the Regulation;
- (b) the Information Notice to be released to customers must clearly explain: 1. the existence of a profiling, providing meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; 2. the data subject's right to object at any time to processing of personal data concerning him or her for profiling purposes;
- (c) the data controller must gather a specific, optional, free, separate (even from the marketing consent) and documented consent to the profiling, revocable at any time. It must also be taken in mind that the European Data Protection Board (a new entity provided by the GDPR) has the specific task to issue (future) guidelines, recommendations and best practices for further specifying the criteria and conditions for profiling data processing.

SBC: What will happen if an operator needs to share customer data with organisations outside the EU?

AdN: Cross-border and international data flows are carefully regulated by the GDPR, if the destination country is not a EU Member State or a non-EU Member State for which a so called adequacy decision as enacted by the EU Commission is not into force (currently, the transfer of personal data towards the following countries is considered as an intra-EU transfer, so no particular issues arises: Argentina, Australia, Canada, Israel, New Zealand, Uruguay, Swiss Confederation and others).

Summarising the main requirements to lawfully transfer personal data abroad to non-EU countries, I may list the following:

- (a) a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection and such a transfer shall not require any specific authorisation;
- (b) in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards may be provided for, without requiring any specific authorisation from a supervisory authority, by:

– the so called binding corporate rules (meaning personal data protection policies which are adhered to by a controller or processor established in the EU for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity);

– the so called data transfer agreements based on the standard data protection clauses adopted by the EU Commission or adopted by a supervisory national data protection authority;

– an approved code of conduct or an approved certification mechanism with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In the absence of all the requirements above, transfers of personal data to a third country or an international organisation may also take place only on specific conditions, amongst which it is worth reminding:

- (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

- (d) the transfer is necessary for important reasons of public interest;
- (e) the transfer is necessary for the establishment, exercise or defence of legal claims.

Finally, where a transfer cannot be based at all on any of the above, it may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data (and in such cases the controller must inform the supervisory authority of the transfer and must specifically and additionally inform the data subject of the transfer and on the compelling legitimate interests pursued).

A particular remark must be made about data transfers to U.S. The EU-U.S. Privacy Shield Framework is an agreement designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce (see the official web site for an overview: https://www.privacyshield.gov/Program-Overview).

SBC: Does the GDPR do anything useful for the industry? Or is it just more red tape?

AdN: As I said before, the GDPR must be approached also as an important chance. First of all the GDPR introduces a more coherent and uniform data protection framework in the European Union (instead of several different national legislations arisen from the different choices of national implementation of the EU Directive 46/95). This shall make easier – even for the Industry – to govern within a certain legal framework the rapid technological developments and globalisation which have brought new challenges for the protection of personal data and an enormously increased capacity to collect and share personal data. Let's say that the GDPR – by providing legal certainty and transparency for economic operators – pursue two main goals: ensuring a consistent level of protection for natural persons and preventing divergences hampering the free movement of personal data within the internal market.

Then, I also think that the "red tape" approach to the GDPR must be excluded: the real "philosophy" basing the Regulation can be read therein: "the proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data".

To make a practical example – amongst the others – of how economic operators may benefit of the new rules (in terms of simplified fulfilments), the new principle called "one-stop shop mechanism" may be referred. It is a mechanism that, in important transnational cases, establishes the "one-stop-shop" in order to arrive at a single data protection supervisory authority decision, which shall be fast, ensure consistent application, provide legal certainty and reduce the administrative burden. This is an important factor to enhance the cost-efficiency of the data protection rules for international business, and so to contribute to the growth of the digital economy.

SBC: What happens to operators who do not manage to fulfil these obligations? Are they answerable to the local regulator? What would be a typical punishment?

AdN: The risks connected to a breach of the obligations set forth in the GDPR may be evaluated at a different levels. The first level relates to the sanctions provided by the GDPR: infringements are subject to administrative fines (imposed by the national data protection supervisory authority) up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, in the most serious cases (administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, can be applied in other cases of breach).

Obviously the fine applied within the single case shall be the result of particular case-by-case evaluations carried out by the national authority according to the parameters set forth within the GDPR (ex: the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; the intentional or negligent character of the infringement; any action taken by the controller or processor to mitigate the damage suffered by data subjects; any relevant previous infringements by the controller or processor; etc ect).

On a different level, beyond the financial impacts of administrative fines as a such, it must be also reminded that any person who has suffered material or non-material damage as a result of an infringement has the right to receive compensation from the controller or processor for the damage suffered, on a civil or tort ground. And a customer damaged for unfair data processing, is a customer lost who probably shall spread in the market a non positive image of that data controller…

Finally, a different level can be that of the impact on operational activities of the economic operators: let's think about a data processing block or suspension orders issued by the supervisory authority as a result of a complaint lodged by a customer or of an investigation carried out by the supervisory authority on its own motion.

Professor Alessandro Del Ninno will be presenting his session on the first day of the Betting on Football Conference next week at Stamford Bridge. Sign up **here** for a ticket.

Data Protection: Marketing and operational implications of the new rules
The enacting of the EU General Data Protection Regulation ("GDPR", applicable starting from May 25th, 2018) is set to have a significant impact and betting and gaming companies need to be gearing up now for the new privacy rules. The paper shall outline the main practical fulfillments to be complied with by betting and gaming companies when processing personal data.

Tagged with: #BOFCON2017 | BETTING ON FOOTBALL CONFERENCE | DATA PROTECTION | DPR | EU GENERAL DATA PROTECTION REGULATION | TONUCCI & PARTNERS

« Previous: Ladbrokes Coral restructures senior legal executive team

Next: New Era as DCMS passes new Horserace Betting Levy into law »

RELATED NEWS

OtherLevels – Sponsor Profile – #bofcon2017
April 24, 2017

140 world class speakers confirmed for Betting on Football
April 24, 2017

OPTIMA – Sponsor Profile – #bofcon2017
April 21, 2017