HFN Technology & Regulation Client Update

February 2019

Dear Clients and Friends,

We are pleased to present the latest edition of our monthly **Technology & Regulation Client Update**, which includes a variety of notable regulatory and industry compliance developments in the fields of personal data protection, cybersecurity, digital advertising and content regulations, internet platform compliance policies and more. These include the following:

- **The UK's new regulations to guide companies on the Post-Brexit** data protection regime;
- **Guidelines on GDPR Codes of Conduct**, published by the European Data Protection Board;
- Guidelines on Artificial Intelligence and data protection, published by the Council of Europe;
- The New York Attorney General's **settlement with a seller of fake followers and likes in social media**, in which the practice was declared as being illegal;
- The UK's advertising regulator's new regulatory guidance the aim of which is to **protect children from irresponsible gambling ads**;
- Germany's Competition Authority's decision prohibiting **Facebook from combining user data from different sources**;
- Illinois' Supreme Court ruling on the **State's Biometric Information Privacy Act**; and
- The **first reports submitted by signatories of the EU code of practice against disinformation ("fake news")**.

Kind regards,

Ariel Yosefi, Partner
Co-Head - Technology & Regulation Department
Herzog Fox & Neeman

UK Publishes Regulations to Guide Companies on the Post-Brexit Data Protection Regime

TOPICS: Data Protection, GDPR, Brexit, UK, EU

The UK Government has published the Data Protection, Privacy and Electronic Communications Regulations 2019 ("**Regulations**") in order to ensure that the data protection regime will function smoothly once the UK decides on the future of Brexit.

The Regulations amend the EU General Data Protection Regulation ("**GDPR**"), such that it can be incorporated into UK domestic law. The Regulations will come into effect on either 30 March 2019, if there is a 'no deal' Brexit; or at the end of the transition period (1 January 2021 at the earliest), if the UK and the EU approve the draft Withdrawal Agreement, which is currently under discussion in the UK Parliament.

The data protection standards set by the UK under the Regulations ("**UK GDPR**"), as well as in the GDPR, are essentially the same. The UK GDPR will apply to any controllers and processors established in the UK and to those outside of the UK, offering goods and services to data subjects in the UK or monitoring the behavior of data subjects in the UK.

Key points include the fact that companies subject to the UK GDPR may need to appoint a UK representative; and that UK's ICO will make its own adequacy decisions with respect to third countries (including EU Member States) in order to permit the transfer of personal data.

On this topic, the **European Data Protection Board ("EDPB") also released an information note addressed to commercial entities and public authorities on data transfers under the GDPR in the event of a 'no-deal' Brexit.** According to the EDPB, in the absence of an agreement between the EU and the UK, the UK will become a third country on 30 March 2019. **Consequently, the transfer of personal data from the EEA to the UK will have to be based on data sharing agreements, codes of conduct or other specific transfer instruments**.

As regards data transfers from the UK to the EEA, according to the UK Government the current practice, which permits personal data to flow freely from the UK to the EEA, will continue in the event of a 'no-deal' Brexit.

We will be happy to provide further advice on how to adapt to UK's new Exit Regulations and other points of attention.

European Data Protection Board Publishes Guidelines on GDPR Codes of Conduct

TOPICS: Data Protection, GDPR, Codes of Conduct, European Data Protection Board

The EDPB published Guidelines regarding the provisions under Articles 40 and 41 of the GDPR, with respect to **Data Protection Codes of Conduct.**

According to the EDPB, **Codes of Conduct represent a practical, potentially cost-effective and meaningful method to achieve greater levels of consistency of protection for data protection rights**, and can help to bridge the harmonization gaps that may exist between Member States in their application of data protection law. Codes may also prove to be a significant and useful mechanism in the area of international transfers, as

new provisions in the GDPR allow third parties to adhere to approved codes in order to satisfy legal requirements for international transfers of personal data to third countries**.**

The Guidelines are intended to **help clarify the procedures and the rules involved in the submission, approval and publication of codes** at both a National and European level. They intend to set out the minimum criteria required by a Competent Supervisory Authority before carrying out an in-depth review and evaluation of a code.

GDPR codes are voluntary accountability tools, which set out specific data protection rules for categories of controllers and processors. They can be a useful and effective accountability tool, providing a detailed description of what is the most appropriate, legal and ethical set of behaviors of a sector. As an example, the Guidelines cite micro enterprises involved in similar health research activities, which could come together via their relevant associations and collectively develop a code in respect of their collection and processing of health data.

A code must be submitted by an association/consortium of associations or other bodies **representing categories of controllers or processors (code owners)** in accordance with Article 40(2) of GDPR. Code owners would include, for example, trade and representative associations, sectoral organizations and interest groups. They can have national or transnational reach, broader or narrower scopes, and **must provide mechanisms that will allow for effective oversight**.

Codes are one of a number of voluntary tools that can be used to assist organizations in demonstrating their compliance with the GDPR. Additional tool is Data Protection Impact Assessments (DPIAs), and a special update we recently published on regarding DPIAs is available here.

Council of Europe Releases Guidelines on Artificial Intelligence and Data Protection

TOPICS: Artificial Intelligence, Data Protection, European Convention on Human Rights, EU

The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("**Convention 108**"), has released **Guidelines on Artificial Intelligence and Data Protection, the aim of which is to provide a set of baseline measures in order to ensure that AI applications do not override human rights, especially personal data privacy rights**.

Convention 108 is the first international agreement dealing with the collection and processing of personal data, and as of now, has been ratified by 53 countries, including non-members of the Council of Europe. Convention 108 reflects new technologies and incorporates regulatory developments. Within the framework of this Convention, the Consultative Committee has released Guidelines on specific topics.

These Guidelines recognize the importance of AI technologies to society, whilst asserting that **the right to protection of personal data is essential when developing or adopting AI applications, in particular when used in decision-making processes**. In this regard, the development of AI technologies should be based on the principles of Convention 108+, considering certain principles, including fairness, purpose specification, proportionality of data-processing, privacy-by-design and by default, responsibility and demonstration of compliance (accountability), transparency, data security and risk management.

According to the Guidelines, **AI developers, manufacturers and service providers should take a number of measures** including:

(i) adopting a **human rights by design** approach and avoiding any potential biases;
(ii) allow meaningful **control by data subjects** over the data processing and the related effects on individuals and on society;
(iii) assessing the **quality, nature, origin and amount of personal data** which is used, and reducing unnecessary, redundant or marginal data, using synthetic data whenever possible;
(iv) setting up consulting independent committees of experts to contribute in order to **detect potential bias**; and
(v) ensuring that individuals have the **right to object** when technology might influence opinion or personal development.

The Guidelines also contain specific recommendations for policymakers and legislators, such that public procurement procedures should impose specific duties of transparency on AI suppliers, prior assessment of impacts on human rights, and vigilance as to the possible adverse effects of AI applications. Furthermore, supervisory authorities should be consulted when AI applications have the potential to significantly impact the human rights and fundamental freedoms of data subjects.

New York's Attorney General Announces a Settlement with Seller of Fake Followers and Likes in Social Media, Declaring the Practice Illegal

TOPICS: Social Media, Fake Followers, Bots, New York's Attorney General, US

The New York Attorney General's ("**NYAG**") office has announced a settlement with the now-defunct company Devumi, which sold **fake followers, "likes" and views on social platforms** such as Twitter, YouTube, LinkedIn, SoundCloud and Pinterest, using activity derived from fake accounts.

In what is the first finding by a law enforcement agency indicating that such activity constitutes illegal deception and illegal impersonation, the NYAG has stated that selling fake social media engagement and using stolen identities to engage in online activity is illegal.

Devumi's practices were first exposed in a New York Times article. The company sold the activity of fake accounts operated by computers - known as “bots” - or by one person pretending to be many other persons, known as “sock-puppet” accounts. Some activity also originated from fake accounts that copied real people's social media pictures and profiles without the knowledge or consent of the user. This, coupled with the fact that Devumi sold endorsements from social media influencers, without disclosing that the influencers had been paid for their recommendations, was considered to be especially troubling, particularly given that the opinions of influencers can have a marked influence on the reputation and sales for any product, company, service or person they endorse (in this regard, please see our special Client Update concerning influencer marketing).

According to the statement released by NYAG, "*with this settlement, we are sending a clear message that anyone profiting off of deception and impersonation is breaking the law and will be held accountable.*" The NYAG’s position demonstrates the importance, which they attach to companies providing services in social media boosting, or using such services, paying special attention to factors such as use of bots and fake profiles.

We will be happy to provide further advice on how to provide or use social media boost services in a lawful way, minimizing compliance risks.

UK Advertising Regulator Publishes Guidance to Protect Children from Irresponsible Gambling Ads

TOPICS: Advertising, Online Gambling, Advertising Standards Authority, UK

The UK's Advertising Standards Authority ("ASA") has published new Guidance on Protecting Children and Young People from **irresponsible gambling ads**, to come into force in April 2019.

The new Guidance prohibits targeting online ads for gambling products at groups of individuals who are likely to be under 18, while **extensively listing unacceptable types of content**, including certain types of **animated characters**, licensed **characters from movies or TV, and sportspeople** and **celebrities who are likely to be of particular appeal to children**. Ads using celebrities or influencers who are, or appear to be, under 25 are also prohibited.

The Guidance also adds to existing guidance on the responsible targeting of ads, covering all media, in order to assist advertisers in understanding what they need to do in order to avoid the under-18s from being targeted with such ad.

In previous recent updates, we also covered UK's CAP rules on the use of personal data for marketing, new standards on gambling advertising in the UK, and the new rules on advertising enforcement.

We would be happy to advise our clients and to clarify the implications arising from the new Guidance.

Germany's Competition Authority Prohibits Facebook from Combining User Data from Different Sources

TOPICS: Data Protection, Competition Law, Facebook, Germany

Germany's Competition Authority ("the **Bundeskartellamt**") has imposed far-reaching restrictions in the processing of user data on Facebook.

According to Facebook's terms and conditions, users will need to provide their consent in order for Facebook to collect the user's data outside of Facebook's website, via the internet or on smartphone apps, and to assign such data to the user's Facebook account.

However, according to the Bundeskartellamt's decision, given Facebook's dominant position in the German market for social networks, which is indicative of a monopolization process, Facebook becomes **subject to specific obligations under competition law**, given that users cannot on a practical level, switch to other social networks. In this regard, an obligatory tick box agreeing to the company's terms of use is not considered an adequate basis for such intensive data processing.

The Bundeskartellamt calls attention to the fact that Facebook collects a massive amount of data from third-party websites with an embedded "Like" button, even if no Facebook symbol is visible. By combining data

from its own website, company-owned services and the analysis of third party websites, Facebook obtains very detailed profiles of its users, who have no choice but to consent to this practice.

In accordance with the Bundeskartellamt's decision, the extent to which Facebook collects, merges and uses data in user accounts, constitutes an abuse of a dominant position.

As such, **the Bundeskartellamt has imposed the following restrictions on Facebook's processing of user data**:

(i) Facebook-owned services, such as WhatsApp and Instagram, can continue to collect data. However, such data can only be assigned to Facebook user accounts subject to the users' voluntary consent. Where consent is not given, the data must remain with the respective service and cannot be processed in combination with Facebook data;
(ii) Collecting data from third party websites and assigning them to a Facebook user account will also only be possible if users have given their voluntary consent; and
(iii) If consent is not given for data from Facebook-owned services and third party websites, then Facebook will have to substantially restrict its collection and combining of data. Facebook is to develop proposals for solutions to this effect.

Illinois Supreme Court Upholds State's Biometric Information Privacy Act

TOPICS: Data Protection, Facial Recognition, Biometrics, Illinois, US

The Illinois Supreme Court recently ruled **that an individual does not need to allege or prove actual injury or adverse effect, beyond mere violation of his or her rights, in order to qualify as an "aggrieved" person and be entitled to seek damages pursuant to the Illinois Biometric Information Privacy Act** ("**BIPA**").

The BIPA, enacted in 2008, regulates "*the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information*", including **fingerprints and facial recognition model**.

The BIPA imposes several obligations on entities collecting, retaining, and disclosing biometric data, including the need to **inform the individual or the individual's representative in writing** that biometric data is being collected or stored and the **purpose** and **length** of term of collection, storage and use of the biometric data. As part of the BIPA's enforcement mechanism, "aggrieved" parties are granted a private right of action and entitled to damages.

In the current case law, the plaintiff claimed that Six Flags, a regional theme park, collected her son's biometric data during a school visit without obtaining prior written active consent or parental notification. Six Flags sought to dismiss the action by arguing that in order to bring a claim as an "aggrieved" party under the statute, the plaintiff was required to allege actual injury or harm beyond the statutory violation.

The Illinois Supreme Court unanimously found that the term "aggrieved" does not require an allegation of actual harm beyond a violation of the rights conferred by the BIPA, since the entity's violation of the BIPA, "*the right of the individual to maintain [his or] her biometric privacy vanishes into thin air . . .*" constitutes an injury that is "*real and significant*."

This ruling demonstrates the importance of strict compliance with the BIPA, in light of the liability to which companies might be subject, ranging from $1,000 to $5,000 per violation.

We would be happy to provide advice and recommendations concerning compliance with collection and usage of biometric data and other sensitive information.

European Commission Receives First Reports Submitted by Signatories of the Code of Practice Against Disinformation

TOPICS: Disinformation, EU Code of Practice against Disinformation, Europe

The European Commission has published the first reports submitted by signatories of the Code of Practice against disinformation, which was signed in October 2018, while calling on signatories to intensify their efforts in the run up to the 2019 EU elections.

The monitoring of the Code of Practice is part of the Action Plan against disinformation, which the European Union adopted in December 2018, in order to enhance its capabilities and strengthen cooperation between Member States and EU institutions, the aim of which is to proactively address the threats posed by disinformation. The Code marks the first time that industry has agreed, on a global and voluntary basis, to self-regulatory standards in order to combat disinformation.

Facebook, Google, Twitter, Mozilla and some additional members of the EDIMA trade association, are among those that have signed the self-regulatory Code, having agreed to submit periodic reports on measures taken in order to comply with the Code. These are the first monthly reports, to be followed by similar reports every month until May 2019. By the end of 2019, the Commission will carry out a comprehensive assessment at the end of the Code's initial 12-month period. Should the results prove unsatisfactory, the Commission may propose further actions, including those of a regulatory nature.

We have included details regarding the provisions of the Code in our previous update, and will monitor any further developments.