HFN Technology & Regulation Client Update

August 2018

Dear Clients and Friends,

We are pleased to introduce you to our new edition of the Technology & Regulation Client Update, which includes notable regulatory and industry compliance developments from the past month, in the fields of privacy and data protection, cyber-security, digital advertising, content and app compliance.

These include the following:

- **GDPR compliance warnings by the French Data Protection Authority concerning the collection of personal information by digital advertising SDKs;**
- **Regulatory developments in the UK and Italy on advertising online gambling;**
- **The continuing data privacy and protection trend in the US: the new Ohio Data Protection Act and updated Privacy Shield regulatory guidelines; and**
- **The entering into force of the next stage of the New York Financial Services Cybersecurity Regulation.**

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

If you have an important regulatory or industry compliance update you would like to share with the industry, let us know

French Data Protection Issued Warnings to SDK Companies for Not Complying with the GDPR

TOPICS: Personal Information, Digital Advertising, Mobile, General Data Protection Regulation, France

The French Data Protection Authority ("CNIL") has issued a formal warning to two digital advertising companies for breaching their obligations to obtain consent under the General Data Protection Regulation ("**GDPR**"). Both companies, Fidzup and Teemo, offered **SDK tools which are integrated into the mobile application** code of their customers, mobile app operators. These tools allowed them to collect **geolocation data** and **advertising ID** from smartphone users, even when the application is not running in order to display targeted advertising to users based on the places they visited.

Both companies relied on the users' consent obtained by the mobile app operators to process their personal data, and accordingly, required them to inform users as to the targeted advertising activities and obtain their consent.

However, the CNIL found that **the consent was not obtained in accordance with the GDPR requirements**, based on the following reasons:

- **Informed**: the GDPR requires the consent to be "informed", while in this case, the information, which was for the purpose of collecting the personal information, was provided to users only after the app was installed, when the geolocation data and advertising ID had been already collected. Additionally, for existing apps of new customers, the SDK tool started to apply although the users were not proactively informed regarding the changes to the app's privacy policy or terms of use;

- **Freely Given**: the consent was not "freely given", as required by the GDPR, since the users did not have any alternative but to download the app with the SDK tool; and

- **Specific**: the consent was found not to be sufficiently specific, since the app operators request one single consent, which covered all data processing conducted by them and by the respective SDKs.

Additionally, the CNIL found that Teemo retained the geolocation data for 13 months, which is **contrary to their obligation under the GDPR to define a data retention period that is proportionate to the purpose of processing**, in this case, providing targeted advertising.

We would be happy to advise our clients and clarify the implications arising from this decision.

UK Gambling Commission Announces New Advertising Enforcement Rules

TOPICS: Gambling Advertising, Digital Advertising, UK Gambling Commission, United Kingdom

The UK Gambling Commission has updated its Licence Conditions and Codes of Practice (LCCP) for online gambling operators in relation to **marketing and advertising, unfair terms and the handling of customer complaints and disputes**.

The updated rules, **set to be implemented on 31 October 2018**, will enable the Commission to enforce penalties against operators, who breach the UK's advertising codes, legal requirements to obtain consent in some cases for direct electronic marketing, and consumer protection laws, in order to provide stronger protection for consumers and to ensure they are treated fairly as gambling businesses. This is part of the UK regulators' efforts to enforce strict regulatory standards on advertising that targets gambling (see our related update regarding UK Committee of Advertising Practice's ("**CAP**") standards on the advertising of gambling here).

The key changes of the updated LCCP on digital marketing and advertising include the following:

- Licensees are required to comply with the CAP advertising codes and the Broadcast Committee of Advertising Practice, as applicable. In practice, this means that **these codes of conduct would become an integral part of the gambling licensing conditions**;
- **Licensees are obliged to ensure that their marketing communications, advertisements, and invitations to purchase are not misleading,** that marketing incentives are provided transparently and prominently to consumers and that their **terms and conditions for each marketing incentive are made available**; and
- Unless expressly permitted by law, **consumers must not be contacted with direct electronic marketing without their informed and specific consent**. In this regard, whenever a consumer is contacted, the consumer must be provided with an **opportunity to withdraw his consent**. If consent is withdrawn, then the licensee must, as soon as practicable, ensure the consumer is not contacted with electronic marketing thereafter unless the consumer has one again provided his consent. **Licensees must be able to provide evidence which establishes (i.e. evidences) that consent**;

We would be happy to provide further advice and recommendations concerning the new rules and their implementation.

New Data Protection Act in Ohio

TOPICS: Personal Information, Data Protection, Cyber-Security, Ohio, United States

This month, **Ohio has joined California, Colorado and Vermont, in the new legislative trend of revising US state law on data protection and privacy** (see our previous related update here).

On 3 August 2018, the Governor of Ohio signed into law the Ohio Data Protection Act which offers "safe harbor" to companies that meet cyber standards. The new law will take effect 90 days after it is provided to the Ohio Secretary of State.

A covered entity under this law is any business that accesses, maintains, communicates, or processes personal information or restricted information in or through one or more systems, networks, or services, whether or not located in Ohio. **The law provides these businesses with an affirmative defense** to tort claims based on Ohio law or brought in an Ohio court in relation to data breaches, **provided that the business was in compliance with reasonable security measures, as specified in the law, at the time of the breach**.

In order to be entitled to the affirmative defense, **a covered entity must demonstrate that it created, maintained, and complied with a written cybersecurity program for protection of personal information**, that:

- **Conforms to certain industry-recognized cybersecurity frameworks**, such as the Health Insurance Portability and Accountability Act ("HIPAA"), Gramm-Leach Bliley ("GLBA"), and PCI DSS;
- **Was designed to protect the security and confidentiality of the information**, to protect against anticipated threats or hazards to the security of integrity of the information and against unauthorized access to the information; and
- **The scale and scope of the cybersecurity program is considered appropriate,** based on the size and complexity of the entity, its nature and scope of activities, the sensitivity of information that needs to be protected and the cost and availability of tools to improve information security.

We will be happy to advise our clients and clarify the overreaching implications of this new legislation, as well as the other new requirements in the US.

Asia House, 4 Weizmann St., Tel-Aviv 6423904, Israel | Tel: (972)-3-692-2020 | Fax: (972)-3-696-6464
Twitter: @hfnlaw | Blog: unfolding.co.il | hfn@hfn.co.il | www.hfn.co.il

Italian Parliament Bans all Forms of Gambling Advertising

TOPICS: Gambling Advertising, Digital Advertising, Italy

The Italian Parliament passed a new law called the "Dignity Degree", which includes a prohibition against all gambling-related advertising in the country. The new law also prohibits all sports sponsorships provided by gambling companies. Failure to comply with this law will result in administrative fines up to 5% of the value of the advertising or sponsorship for each violation, and in cases of advertising gambling services or products to children, even a larger fine.

Effective 1 January 2019, all gambling ads will be immediately removed from the radio, TV and the Internet. However, the legal framework has taken into account cases of companies that have existing contracts to fulfill, and in this regard, they will be given until 30 June 2019 to comply with the law. A number of gambling companies in Italy have voiced their objection to the blanket ban on advertising, arguing it will encourage illegal gaming.

New Privacy Shield Guidelines published by the US Department of Commerce

TOPICS: Personal Information, Privacy Shield, European Union, United States

The US Department of Commerce has updated its frequently asked questions ("FAQs") regarding the EU-US and Swiss-US Privacy Shield Frameworks ("Privacy Shield"), in order to shed light on additional matters under the Privacy Shield framework, specifically following the implementations of the GDPR across the EU.

The key additions to the FAQs are:

- **Processing**: the Department of Commerce has clarified in its **processing guidance** that when responding data subjects seek to exercise their rights under the Privacy Shield Principles, the processor must comply according to the instructions of the EU data controller. For instance, in order to comply with the right of access, the processor who participate in the Privacy Shield, should provide access by ensuring that the individual is put in contact with the EU controller, or by working with the EU controller to provide access, as prescribed by the EU controller;

- **Onward Transfer**: the FAQs now include a dedicated guidance for organizations that wish to comply with the **Accountability for Onward Transfer Principle**. This guidance states that a contract with controllers and agents is not always required when transferring data to them. For example, in cases of occasional employment-related

operational needs that involve their personal information, a contract will not be needed when the transfer is limited to a small number of employees; and

- **CLOUD Act**: the FAQs states that the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), which involves data transfers for law enforcement purposes, does not conflict with the Privacy Shield and has no effect on it.

The New York Department of Financial Services Reminds Entities of Upcoming Compliance Date for its Cybersecurity Regulation

TOPICS: Cybersecurity Regulation, Department of Financial Services, Data Protection, New York, United States

The New York State Department of Financial Services ("DFS") has issued a regulatory reminder, according to which, the next compliance date for its Cybersecurity Regulation is 4 September 2018.

The Regulation was published in February 2017 (see our previous related report here), requiring banks, insurance companies and other financial services institutions that are regulated by the DFS ("**covered entities**"), to **establish and maintain a cybersecurity program that protects their consumers' personal information and ensures their safety and soundness**.

Pursuant to the Regulation's implementation deadlines, **all covered entities will have to comply with the following requirements by 4 September 2018:**

- **Audit Trail**: all covered entities must securely maintain systems to facilitate reconstruction of material financial transactions and cybersecurity audit trails and retain related records for a period of three to five years. Covered entities are also required to have audit trails that are able to detect and respond to cybersecurity events;

- **Application Security**: covered entities are required to maintain security programs that include written procedures, guidelines and standards in order to ensure they use secure practices, as well as procedures for evaluating and assessing the security of externally-developed applications utilized by them;

- **Data Retention Limitations**: all covered entities are required to have policies and procedures for the secure disposal of non-public information that is no longer needed for the business operations or other legitimate purpose, unless they are required to retain it by another law or regulation;

- **Training and Monitoring**: the regulation requires all covered entities to implement risk-based policies, procedures and controls designed to monitor the activity of authorized users, in order to help detect unauthorized access or use of nonpublic information; and

- **Encryption of Nonpublic Information**: covered entities must implement systems that can encrypt nonpublic information to protect that data from unauthorized access, disclosure, or destruction.

Additionally, the DFS reminds covered entities that they have until 1 March 2019, to assess the risk that third-parties services providers might cause to their systems, and to ensure that they are protected.