HFN Technology & Regulation Client Update

June 2018

Dear Clients and Friends,

We are pleased to present our June edition of the Technology & Regulation Client Update, which includes several notable regulatory and industry compliance developments in the fields of data protection, digital advertising, content, security and app compliance.

These include the following:

- **Facebook Page Administrator Responsible for Data Processing;**
- **The new European Data Protection Board Updated Guidelines on GDPR;**
- **Apple's Revised Guidelines for App Store on Cryptocurrency and Contacts Data;**
- **Google Blocks Inline Installation of Chrome Extensions;**
- **The Israeli Prime Minister's Office Presentation of a New Cybersecurity Bill;** and
- **The US Supreme Court's Ruling on Digital Privacy.**

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, please let us know

Facebook Page Administrator Responsible for Data Processing

TOPICS: Data Protection, Facebook, Court Ruling, Court of Justice, General Data Protection Regulation, European Union

The EU Court of Justice (ECJ) ruled that the administrator of a Facebook page is jointly responsible, together with Facebook, as joint data controllers.

In this case, a German company was the administrator of its fan page on Facebook. As the administrator, this company could obtain anonymous statistical data on visitors to its fan page via the "Facebook Insights" function, which enables the storage of cookies on visitors' hard drives in order to collect data about them.

The German Supervisory Authority ordered the administrator to deactivate the page due to lack of transparency for the users. Although the company argued that it was not responsible, **the ECJ ruled that the page administrator was a data controller since it takes part in the determination of the purposes and the means of processing of the visitors' personal data**. **Accordingly, the ECJ found both Facebook and the page administrator responsible, as joint data controllers**.

The ECJ also noted that via Facebook Insights tool, administrators could ask for information which helps them decide which offers they should make based on the users' information. **The fact that an administrator of a fan page uses Facebook's platform in order to benefit from its services, cannot absolve it from any liability with respect to the protection of personal data.**

Although this judgment was based on an analysis of the EU's Privacy Directive 95/46, which has now been replaced with the General Data Protection Regulation ("**GDPR**"), the terms and concepts in this area remain unchanged, and consequently, it adds important details with regard to the roles of a data controller and data processor.

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

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

European Data Protection Board Updated Guidelines on GDPR

TOPICS: Data Protection, General Data Protection Regulation, ePrivacy Regulation, European Data Protection Board, European Union

With the GDPR having come into force, the European Data Protection Board (EDPB) replaced Article 29 Data Protection Working Party ("WP29") (for more information concerning this replacement, see our related update here) as the EU data protection advisory regulator.

The EDPB is an independent European body, whose purpose is to ensure the consistent application of the GDPR and the EU Law Enforcement Directive, as well as promoting cooperation between the EU's data protection authorities. The EDPB can adopt general guidance in order to clarify the EU data protection laws, and unlike WP29, **it is also empowered to make binding decisions** in order to ensure consistent compliance accordingly.

Immediately after the GDPR came into force, the EDPB came into effect and took the following steps:

Endorsing WP29 position

The EDPB endorsed many of the previous positions of WP29 on the GDPR, such as:

- Guidelines on **consent** under the GDPR;
- Guidelines on **transparency** under the GDPR;
- **Automated individual decision-making and profiling** guidelines for the purpose of the GDPR;
- **Personal data breach notification** guidelines under the GDPR;
- **The right to data portability** guidelines under the GDPR; and
- **Data protection impact assessment** (DPIA) guidelines and determining whether processing is "likely to result in a high risk" for the purposes of the GDPR.

Draft guidelines on certification and identifying certification criteria under the GDPR

The purpose of these draft guidelines is to explain the **key concepts of the certification provisions** under the GDPR Articles 42 and 43, their scope and purpose and to explore the rationale for certification as an **accountability tool**.

Inter alia, the guidelines state that **the term "certification" under Articles 42 and 43 of the GDPR, shall refer to third party attestation which relates to processing operations by controllers and processors, as well as providing a definition of the terms "certification mechanisms, seals or marks"**, not defined by the GDPR. In addition, the guidelines **explain the obligations of a Supervisory Authority when acting as a certification body, and**

compliance aspects that shall be taken into account when drafting certification criteria, which include the lawfulness of processing, the data subjects' rights and the obligation to notify data breaches.

Adopting the final version of the guidelines on transferring personal data outside of the EEA under the GDPR

These guidelines are aimed at providing guidance as to the application of Article 49 of the GDPR with regard to derogations within the context of **transfers of personal data to countries outside of the European Economic Area** ("EEA"), an international organisation (if an adequate level of data protection is provided for in that country or by that international organisation), if appropriate safeguards have been put in place and unclear data subjects' rights at the level of protection, as guaranteed by the GDPR.

The guidelines, which were founded on the previous work carried out by the WP29, provide clarification as to the following derogations:

- **The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards**: The guidelines focus on the specific elements required for such consent to be valid: consent must be explicit, specific for the particular data transfer/set of transfers and the data subject must be properly informed, particularly as to the possible risks of the transfer;

- **Transfer necessary for the performance of a contract between the data subject and the controller or for the implementation of pre-contractual measures taken at the data subject's request**: The guidelines explain the criterion of "necessity" and of "occasional transfers" which have to be taken into account. The guidelines state that this requires a close and substantial connection between the transfer of data and the purposes of the contract and that whether or not the transfer can be deemed as occasional, will have to be determined on a case by case basis. In this regard, the guidelines set out some examples;

- **Transfer 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**: Similar to the above derogation, the guidelines explain the terms "necessity" and "occasional transfers" within the context of this derogation.

- **Transfer is necessary for important reasons of public interest**: The guidelines state that this derogation only applies when it can be deduced from EU law or the law of the member state to which the controller is subject;

- **Transfer is necessary for the establishment, exercise or defence of legal claims**: The guidelines explain the range of activities that are covered by the term "establishment, exercise or defence of legal claims" and the "necessity" requirement, adding that such transfers should only be made if they are occasional;

- **Transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent**: The guidelines provide several examples to better explain this derogation. For example, the guidelines state that it is possible to transfer personal data if the data subject, whilst outside the EU, is unconscious and in need of urgent medical care, then only an external party (known as a "exporter") – normally the person's usual doctor and who is established in an EU Member State – would be authorised to supply the data;

- **Transfer made from a public register**: The guidelines state that the register must be open to consultation by the public in general or by any person who can demonstrate a legitimate interest. In addition, according to the guidelines, data controllers and data processors who wish to transfer personal data under this derogation must be aware that a transfer cannot include the detailed personal data or entire categories of the personal data contained in the register, and that in each case, data exporters would have to consider the interests and rights of the data subject; and

- **Compelling legitimate interests**: The guidelines explain that this derogation can be used only if the derogations referred to above, cannot be applied. Furthermore, the guidelines provide an explanation of the remaining requirements, such as applying additional measures as safeguards, informing the data subject of the transfer and of the compelling legitimate interests pursued and that only interests that can be recognised as "compelling" are relevant to the scope of this derogation.

Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications

The statement **supports the quick adoption of the proposed ePrivacy Regulation** in light of the increased usage of IP-based communications and the need to ensure end-users' confidentiality of communications. In the statement, the EDPB offers insights and clarifications on key issues, including **preventing the processing of electronic communications on the "legitimate interest" of the data controller or on the general**

purpose of the performance of a contract, and arguing that the use of anonymised electronic communication data should be encouraged.

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

Apple Revises Guidelines for App Store on Cryptocurrency and Contact Info

TOPICS: Data Protection, Cryptocurrency, Initial Coin Offerings, App Industry Compliance, Apple

Apple has recently released an updated version of its App Store Review Guidelines in which two significant changes have been implemented:

Cryptocurrency mining

The updated guidelines were revised to **explicitly ban apps that mine cryptocurrency on Apple's devices**.

By doing so, Apple joins Google, which updated its Chrome Web Store policy to include prohibitions regarding extensions that mine cryptocurrency (see our related update here), and Microsoft, which published that by July 2018, its Bing search engine will ban cryptocurrency advertisements on its platform, as is the case with other internet giants (see our additional related reports regarding similar policy changes by Facebook and Twitter).

The revision includes five rules:

- Apple will allow virtual-currency wallet apps, provided they are offered by developers who are **enrolled as an organisation**;
- The only cryptocurrency-mining apps allowed are **apps that mine outside the device** (such as cloud-based mining);
- Apps may help users make transactions or transmissions of cryptocurrency on an approved exchange, **as long as they are offered by the exchange itself**;
- Apps facilitating Initial Coin Offerings (**"ICOs"**), cryptocurrency futures trading, and other crypto-securities or quasi-securities trading need to be from **established banks, securities firms, futures commission merchants, or other approved financial institutions and must be lawful**; and
- Cryptocurrency apps **may not offer users virtual coins for completing tasks**, such as downloading other apps, encouraging other users to download or posting to social networks.

Phone contacts

In addition, the guidelines were revised to prevent app developers from obtaining data from phone contacts.

The change **is aimed at ending the common practice by which developers have asked users for access to their phone contact list, which contains phone numbers, email addresses and profile photos. The developers used this information for marketing, and in some cases even shared or sold the information without having obtained any permission to do so from these persons**.

The changes in the guidelines explicitly state that **developers cannot build a contact database using information gathered from users' contacts or contact people using information collected through accessing a user's contacts list**.

We would be happy to advise on any questions that may arise from the new Apple's App Store Guidelines changes.

Google Blocks Inline Installation of Chrome Extensions

TOPICS: Unwanted Extensions, App Industry Compliance, Google Chrome

Google has recently announced that it will stop support for inline installations of Chrome extensions from outside websites. This means that users will only be able to install extensions from the Chrome Web Store. This step was taken by Google as part of an ongoing attempt to ensure choice and transparency to its users.

Google stated that the descriptions displayed alongside extensions in the Chrome Web Store are instrumental in helping people make informed decisions on whether or not they wish to install an extension. **Google found that when comparing extensions installed through inline installation, users are less likely to uninstall or complain with regard to a confusing or deceptive description if the installation came from the Chrome Web Store.**

Google has begun to enforce the new rule by automatically blocking the inline installation function for all extensions initially published on the 12th of June 2018 or later. After the 12th of September 2018, inline installation will be **disabled** for existing Chrome extensions, and finally, in early December 2018, Google will have completely disabled the inline install API method from Chrome 71.

The Israeli Prime Minister's Office Presented a New Cybersecurity Bill

TOPICS: Cybersecurity, Israeli National Cyber Directorate, Israel

The Israeli Ministry of Justice has published a memorandum of a proposed **National Cybersecurity Bill** **("the Bill") for public comments**, following which it will be presented to a vote in the Israeli Parliament (the Knesset).

The preamble to the Bill states that **there is a significant increase in the frequency of cyber threats the aim of which is to harm public safety, the economy and homeland security, and accordingly, national involvement is needed**. **The Bill establishes the foundations for cooperation between the Israeli Government and civil organisations in order to protect cyber-space** and will apply to government offices, critical infrastructures, and civilian entities. The Bill emphasises the importance of the balance between protection of the public in the cybersecurity sphere, and avoiding overloading the economy with a layer of bureaucracy.

The Bill also establishes a framework for the roles and powers of the Israeli National Cyber Directorate, defining it as a security organisation within the Prime Minister's Office, the **purposes of which are to protect the Israeli cyber-space and promote Israel as a world leader in the cyber field.** Inter alia, **the National Cyber Directorate will manage and operate national defense actions against cyber-attacks and promote international cooperation in the cyber field.** According to the Bill, the National Cyber Directorate will be authorised to instruct organisations on how to act in cases of data breach or if there is a suspicion of hacking, and that in any event, those organisations will be required to maintain the confidentiality of those instructions.

The Bill also establishes a regulatory authority dedicated to the cybersecurity field, since the State has a great responsibility in the prevention and preparation for cyber-attacks, as explained in the preamble. Among its other responsibilities, the Bill states that this authority will classify the organisations under its supervision according to the damage to which they are exposed in cyber-attack scenarios, and instruct them to carry out certain actions in order to minimise it.

The Bill has been widely criticised for two main reasons: first, **this Bill gives the National Cyber Directorate extended powers to search and seize private computers** from private companies and even from individuals' private houses without a court order, in order to foil or deal with a cyberattack. Secondly, **it enables the Government to collect private data from companies that are responsible for critical portions of Israel's digital and physical infrastructure**, such as internet providers. Critics claim that the Bill raises serious concerns as to the potential of harm to the privacy of Israeli citizens, as well as to trade secrets of private organisations.

US Supreme Court's Ruling on Digital Privacy

TOPICS: Data Protection, US Supreme Court, United States

A new Supreme Court ruling in Carpenter v. United States case imposes limits on police, stating that police must generally obtain a warrant to seize cellphone tower location records.

This case was dealing with the question of whether or not there was a reasonable expectation of privacy when location records were held by third party, such as a phone carrier. The Supreme Court ruled that **obtaining this kind of private data without a warrant from wireless carriers, as police usually do, would be considered as an unreasonable search and seizure under the US Constitution's Fourth Amendment.** The court noted that these records are highly sensitive, in that they provide information as to where a person is located, every day, every moment, and over several years.

Fourteen of the largest US tech companies, including Google, Apple, Facebook and Microsoft were also involved in this case, as they filed a brief in support of neither party. In this brief, they argued that the Fourth Amendment needs to be amended for the digital era. Although the brief was not officially filed in support of either party, **in practice, their opinion was in favour of Carpenter's position, stating that the court should reconsider whether the Government should easily be able to obtain access to that data**.