HFN Technology & Regulation Client Update

October 2017

Dear Clients and Friends,

We are pleased to introduce you to our October edition of the Technology & Regulation Client Update, which includes several important regulatory and industry developments in the fields of data privacy, technology compliance, content, digital advertising and information security regulations. These include the following:

- **Updates to Google Play policies addressing quality requirements, user permissions, ads and gambling apps;**
- **New GDPR guidelines published by the EU data protection advisory body (the Article 29 Working Party), addressing data breach, automated decision making and profiling, administrative fines and data protection impact assessment;**
- **The European Commission's guidance on UGC platform's responsibility with respect to online illegal content;**
- **Google Chrome's new anti-unwanted-software and security feature; and**
- **The UK Government's report on artificial intelligence regulatory oversight.**

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.

Updates to Google Play Policies

TOPICS: App Compliance, Gambling Apps, Content Rating, User Data, Google Play

Recently, Google Play has introduced several important updates to its Developer Program Policies, focusing on functionality and quality requirements, user permissions, ads and gambling apps (see our related report on previous updates to these policies).

Please find below an overview of the key updates:

- For the first time, Google Play has introduced **minimum functionality and quality requirement from apps**, namely that apps must provide a stable, responsive user experience, and should NOT crash, force close, freeze, or otherwise function abnormally (such as apps that do not install, load or are not responsive).

- With respect to **permission requests**, Google has taken additional steps to protect users by limiting how and when developers can make such requests:
  - Apps should not request access to **information that is not needed** for the app's purpose;
  - Apps may only request access to the user data that is necessary to implement **existing features or services** in the app. In other words, app should not attempt to "future proof" access to user data by requesting access to information that might benefit services or features that have not yet been implemented;
  - Permission requests should make sense to users, and should be limited to the **critical information necessary to implement the app**; and
  - Permissions should be **requested in context**, where possible, by using incremental authorizations. In using incremental authorizations, the app initially requests only the scopes which are required to start the app, and then requests additional scopes as new permissions if required, in a context that identifies the reason for the request to the user.

- Guide apps, the **primary purpose of which is to serve ads, are prohibited**.

- With respect to **gambling apps** – gambling apps may not be available in any location other than the UK, France and Ireland.

We would be happy to advice on any questions that may arise regarding the updated policies.

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

The EU's Article 29 Working Party New Guidelines on GDPR

TOPICS: Automated individual decision-making, Profiling, Data Protection Impact Assessment, Administrative Fines, Article 29 Working Party, EU General Data Protection Regulation, European Union

The EU General Data Protection Regulation ("**GDPR**") enters into force in May 2018. As part of the implementation period, the EU's Article 29 Working Party ("**WP29**") has recently issued **key guidelines addressing various key aspects of the GDPR**. Although the WP29's opinions and guidelines are not binding, since it is an advisory body made up of a representative from the data protection authority of each EU Member State, and includes the European Data Protection Supervisor and the European Commission, these guidelines can assist in understanding how European data protection authorities will interpret various requirements of the GDPR.

- The new guidelines include the following:
  - **Guidelines on Data Protection Impact Assessment** ("**DPIA**"), which have been approved as final versions, after examining comments received during the public consultation;
  - Guidelines on **Data Breach Notifications** (adopted and available for public consultation before their final adaption);
  - Guidelines on **Automated individual decision-making and Profiling** (adopted and open for public consultation before their final adaptation); and
  - Guidelines on the **application and setting of administrative fines for the purpose of the GDPR**.

- Additional GDPR-focused guidelines that were previously adopted by the WP29 are:
  - Guidelines on the right to "data portability";
  - Guidelines on Data Protection Officers; and
  - Guidelines for identifying a controller or processor's lead supervisory authority.

Key points related to the new guidelines are as follows:

Guidelines on DPIA

Article 35 of the GDPR requires the use of DPIAs, or risk assessments of the proposed processing of personal data by an organization, as part of regular business processes and the requirement to demonstrate compliance.

In order to provide a more **concrete set of processing operations that require a DPIA due to their inherent high risk**, the WP29 guidelines set out the following set of **risk criteria**:

- **Evaluation and scoring** - Profiling and predicting behaviors;
- **Automated decision-making having a legal or similar significant effect** - profiling which may lead to the exclusion of or discrimination against individuals;
- **Systematic monitoring** – this would include employees' monitoring programs;
- **Processing of sensitive data**;

- **Large scale processing** - the number of individuals, the volume or range of data, the duration of the processing and its geographical extent;
- **Matching or combining datasets**;
- **Processing data of vulnerable subjects** – this would include children, employees, the mentally ill, patients or the elderly;
- **Innovative use of technological or organizational solutions**; and
- **The processing prevents data subjects from exercising a right or using a service or a contract**.

In addition, the guidelines include various examples which illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA. The guidelines emphasize the importance of continuously assessing and reviewing the processing operations as part of controllers' general accountability obligations.

Guidelines on Data Breach Notifications

The GDPR requires data controllers to notify the competent supervisory authority no later than 72 hours after having become aware of a data breach. Under these guidelines, the WP29 explains **that a controller becomes aware of a data breach when the controller has identified the incident and knows that the personal data has been or is being compromised.** Data processors should also immediately notify data controllers of any breaches.

In addition, the guidelines examine cases where **delayed notification** may be allowed; the **information that should be provided** to the supervisory authority; the way to **determine which supervisory authority** should be notified; and additional requirements concerning **communication to the affected data subjects**.

Guidelines on Automated individual decision-making and Profiling

These guidelines include five sections incorporating "best practice" recommendations the aim of which is to assist controllers in meeting the GDPR requirements on **profiling** and **automated decision-making**. These include the following:

- **Definitions** of profiling and automated decision-making, and the GDPR's approach to these concepts;
- Explanation of **key provisions** on automated decision-making under the GDPR (such as prohibition on fully automated individual decision-making, including profiling that leads to decisions **that impact the individual in a sufficiently significant way**; **exceptions** to the prohibition; and the **right of the data subject to be informed** regarding the automated decision-making);
- Explanation of other general requirements of profiling and automated decision-making (including **transparency**; **fairness**; **data minimization**; and **storage limitation**);
- **Children** and profiling; and

- **DPIAs** – the requirement to carry out DPIAs for evaluations based on profiling and automated processing, including profiling having a legal or similarly significant effect that is not entirely automated, as well as in the case where the profiling is solely automated.

Guidelines on the application and setting of administrative fines

Administrative fines are a central element in the new enforcement regime introduced by the GDPR, and the consequences of non-compliance under the new regulation may result in **fines of up to €20 million or 4% of the company's annual global turnover**.

The WP29's guidelines on this subject are directed at the supervisory authorities, to be used by them as part of their enforcement policy. According to the guidelines, data protection authorities ("**DPAs**") should consider the "nature, gravity and duration of the infringement." It is to be noted that under the guidelines, "minor infringements" might only give rise to a reprimand, especially when the infringement does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation in question. In addition, if a fine would impose a "disproportionate burden" on a "natural person," then a reprimand might be appropriate.

The guidelines state that DPAs must assess each case individually in order to identify the most "effective, proportionate and dissuasive" measures. For the purpose of doing so, DPAs are instructed to consider the **following factors** in determining the size of a fine:

- The nature, gravity and duration of the breach;
- The number of data subjects involved;
- The scope and purpose of the processing;
- The damage suffered by data subjects (and any action taken by the organization to mitigate this damage);
- The degree of responsibility of the organization including the technical and organization measures implemented by it;
- The intentional or negligent character of the breach; and
- The degree of cooperation with the DPAs in order to remedy the breach.

If the organization has taken certain actions in order to reduce the consequences of the breach, then the "responsible behavior" will be a consideration in the calculation of the sanction to be imposed.

We would be happy to provide further advice and recommendations concerning the various WP29's guidelines and their scope. For further details and recommendations published by us on the GDPR, see our update on How to prepare to the new EU General Data Protection Regulation, as well as our recent GDPR Compliance Playbook.

European Commission Guidance on Tackling Illegal Content Online

TOPICS: Illegal Online Content, User Generated Content, European Commission, European Union.

Following the increasing public and regulatory concerns regarding illegal, abusive and misleading information which is easily published on **user generated content platforms**, the European Commission recently published new guidance on Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms. The document provides a **set of guidelines and principles directed towards online platforms and their role and responsibilities in dealing with illegal content online**.

Although the guidance neither changes the legal framework and nor is binding, its aim is to guide online platforms in cooperation with national authorities, EU Member States and other relevant stakeholders on the ways by which they can implement the **good practices for preventing, detecting, removing and disabling access to illegal content**, increasing transparency, as well as the protection of fundamental rights. The main elements of this guidance are as follows:

- Online platforms should have the **necessary resources to understand the legal frameworks** in which they operate, and cooperate closely with law enforcement and other competent authorities where appropriate, notably by ensuring that they can be rapidly and effectively contacted for requests in order to remove illegal content;
- Online platforms should **cooperate closely with 'trusted flaggers'** (i.e., specialized entities with expertise and dedicated structures for detecting and identifying such content online). This cooperation should provide for mutual information exchange, thereby expediting the removal process over time;
- Online platforms should deploy **easily accessible and user-friendly reporting mechanisms,** which enable the notification of content, considered to be illegal, that the platforms might host. The mechanisms (through the issue of an appropriate notice), should be sufficiently precise and adequately substantiated in order for the platforms to be able to take a swift and informed decision for any follow up. Users should not be required to identify themselves in the notices, unless this information is required to determine the legality of the content;
- Online platforms should utilize and develop **automatic detection and filtering technologies and adopt effective proactive measures** in order to detect and remove illegal content online, as quickly as possible, and not simply reacting to notices that they receive. Removal on a quick basis is particularly important and can be subject to specific timeframes where serious harm is at stake (e.g., if content is inciting the commission of any terrorist act). If in the context of the removal of illegal content, platforms find evidence of any criminal activity, this should be reported to the law enforcement authorities;
- Online platforms' **term of services should include clearly explained removal policies**. In addition, the platforms should publish periodic **transparency reports** which provide detailed information regarding the number and types of notices they have received;
- Online platforms should **restore the content** that was removed without any undue delay or allow for the re-upload by the user, without prejudice to the platform's terms of service, when a

counter-notice provides reasonable grounds to consider whether or not the notified information or activity is illegal;

- Online Platforms should put in place measures to **dissuade users from repeatedly uploading illegal content**. The guidance also encourages platforms to use and develop automated technologies to prevent the re-appearance of illegal content.

Google Adds Native "Unwanted Software Cleanup" Features in Chrome

TOPICS: App Compliance, Unwanted Software, Google Chrome, Google Safe Browsing

In our pervious updates, we reported on Google's research regarding ad injections and Google's limitations on changing Chrome settings . As part of Google's ongoing efforts to fight ad injection and other potentially unwanted software, the company has introduced new features in Chrome for Windows that will better protect users against the risks of such unwanted and potentially harmful software. The new security features for Chrome on Windows are in addition to existing defenses, such as Safe Browsing warnings for pages known to deliver malware.

Google is now targeting Chrome extensions that change user settings, such as the default search engine, without using the approved API. With this new feature, the browser will automatically detect when an unauthorized change is made and will offer to restore the original settings.

Google has also redesigned Chrome's Cleanup feature which offers a shortcut to restoring the browser's default settings after an infection. It shows an alert when the browser detects unwanted software and offers a way to remove it. Chrome users have previously been able to use the standalone beta tool Chrome Cleanup Tool to remove harmful software, and the company is now saying that it has redesigned the alerts in order to make it easier to see what software will be removed.

Report on the Growing Artificial Intelligence Industry in the United Kingdom

TOPICS: Artificial Intelligence, General Data Protection Regulation, United Kingdom

The UK Government has issued a report advising on how to address legal challenges arising from future artificial intelligence technologies. The report, entitled Growing the Artificial Intelligence Industry in the UK Report has been compiled by more than 100 experts, who have recommended to establish an AI Council that will operate as a **strategic oversight group** and allow an open and non-competitive forum for coordination and collaboration between industry, the public sector and academia.

In the light of the GDPR, that provides the right to data subjects to demand an explanation regarding an algorithmic decision (see our report above regarding automated decision making), the report also recommends creating a process that would enable developers to explain why their AI is behaving in the way it is.

Additionally, the report states that data trusts should be created. These would involve appointing a consultant to advise on how data should be used for the handling of training AI systems. In view of this report, stopping complex incidents of unlawful data sharing deals, may become easier to fulfill.