HFN Technology & Regulation Client Update

April 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 first fine imposed by the Polish Data Protection Authority for **scrapping of personal data;**
- Revised Q&A issued by the European Commission on the **interplay between clinical trials and the GDPR**;
- Guidelines on the use of **performance of contract as a legal basis for processing of data under the GDPR** published by the European Data Protection Board;
- UK ICO's enforcement measures against a company for illegal collection and sharing of personal data for data brokerage;
- An FTC case **challenging online reviews where compensation had been provided**;
- US regulators' warning to **companies advertising cannabidiol (cbd) products**;
- **Series of regulatory innovation programs launched in the EU**;
- UK government's calls **for regulation of online harm** and liability for social media.

Kind regards,

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

Polish Data Protection Authority Penalises Firm for the Scrapping of Personal Data

TOPICS: Privacy, Data Scrapping, GDPR, Polish Data Protection Authority

Poland's Data Protection Authority ("**UODO**") issued its first fine under the General Data Protection Regulation ("**GDPR**"), penalizing a digital marketing company, Bisnode, **for scraping public data of individuals and reusing it commercially without notifying them**.

In the case in question, Bisnode obtained a variety of personal data from public registers and other public databases relating to millions of entrepreneurs and business owners, including personal data containing national ID numbers and business activity, and in addition, where it processed the data for commercial purposes.

However, **it only informed 90,000 of the individuals whose email addresses had been obtained.** The remaining individuals (whose postal addresses and telephone numbers had been disclosed) were not notified directly due to the high operational costs involved, and were notified by way of a general notice on its website instead.

The UODO considered this action an infringement of Article 14 of the GDPR, which **requires controllers to inform anyone whose personal data they intend to process, if their information has not been directly obtained from them**. By failing to directly inform individuals, Bisnode had prevented them from exercising their rights under the GDPR.

Furthermore, the Polish regulator considered that in this case, the infringement was an intentional act on the part of the controller, since the company was aware of the obligation to provide the relevant information. UODO also highlights the fact that of approximately 90,000 people who were informed as to the processing of data by the company, more than 12,000 objected to the processing of their particular data, which underlines the importance of the obligation to provide such information.

Following this decision, Bisnode must either notify all of the remaining individuals through their postal addresses or telephone numbers, or erase the datasets.

The topic of "scrapping" personal data has been a major area of discussion, as demonstrated in two other cases covered in our previous newsletters, Facebook vs. Power and Linkedin vs. hiQ, and which is now raising new questions, as can be seen by the GDPR's regulatory implementation.

We will be happy to provide further advice on scraping of publicly-available personal data and best practices.

European Commission Issues Revised Q&A on the Interplay between Clinical Trials and the GDPR

TOPICS: Privacy, Health Data, Clinical Trials, GDPR, European Commission

The European Commission's Directorate-General for Health and Food Safety, has issued a revised **Q&A** analysing the interplay between the EU Clinical Trials Regulation ("**CTR**") and the GDPR. The

Q&A takes into account the **Opinion** of the European Data Protection Board ("**EDPB**") issued in January 2019, on the same topic.

The CTR is applicable to clinical trials, the purpose of which is to gather reliable and robust data on an investigational medicinal product. In this regard, the CTR imposes a series of standards for clinical trials, which requires the sponsor/investigator to record, process, store and handle data in such a way that it can be accurately reported, interpreted and verified, while preserving the confidentiality of the records and requiring appropriate technical and organisational measures to protect information and personal data. This aligns with the GDPR, whose objective is to ensure that personal data is both protected and transparent (that is, the subject is informed as to what data processing measures are to be taken). It follows that **in the case of clinical trials, the CTR and GDPR apply simultaneously.**

Accordingly, the controller must ensure that the processing operations carried out in the context of a clinical trial, comply with all the data protection rules under the GDPR, as well as also being responsible for ensuring the legal basis for processing data.

The Q&A, as with the EDPB Opinion, **distinguishes between two different processing purposes associated with clinical trials and attributes different legal bases to each**:

i. Processing for **patient safety purposes**, such as safety reporting, archiving and inspections, which is required by the CTR and for which no consent is required, as it is derived from, and based upon, a legal obligation.

ii. Processing for **scientific research purposes**, which arises if controllers consider a number of different legal bases, such as public interest, legitimate interest or participant consent. However, the Q&A notes that consent will not be the appropriate legal basis in most cases, and consequently, controllers must have particular regard to the situation where a subject belongs to an economically or socially disadvantaged group, or is in position of disadvantage.

With regard to the question of consent, the Q&A states that consent for **participation** in a clinical trial should be distinguished from obtaining consent for the **processing** of **personal data** within the context of that clinical trial, since consent under the CTR is not conceived as an instrument for data processing compliance. This is due to the fact that in the case where a participant withdraws his/her consent to the clinical trial, the trial data can still be processed if collected on another legal basis, that does not necessarily constitute consent, such as legal retention obligations.

In addition, the Q&A highlights the fact that the secondary use of clinical trial data for scientific research purposes is presumed to be compatible with its original use, in accordance with Article 5(1)(b) of the GDPR. Consequently, it should not be necessary to obtain a new consent in order to engage in additional secondary research. However, the Q&A indicates that it is advisable for the consent of data processing within a secondary use, to be obtained separately, using different consent sheets, from the outset of the research itself.

Finally, the Q&A also deals with the international transfer of data, and highlights the fact that the GDPR's transfer restrictions also apply to transfers of clinical trial data.

We would be happy to provide further advice on all aspects concerning the interplay between HealthTech and data regulations.

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

European Data Protection Board Publishes Guidelines on Use of Performance of Contract as a Legal Basis for Processing of Data

TOPICS: Privacy, Legal Basis for Processing, GDPR, EDPB

The EDPB has issued Guidelines on the applicability of Article 6(1)(b) of the GDPR, which provides a lawful basis for the processing of personal data, to the extent that the processing is **necessary for the performance of a contract**. The aim of the Guidelines is to ensure that this **lawful basis is only relied upon where appropriate, especially within the scope of online services.**

According to Article 6(1) of the GDPR, the processing of data shall be lawful only if it complies with any of the six specified conditions set out in this Article, one of which (Article 6(1)(b)) is where the processing is necessary for contractual performance or in order to take steps prior to entering into a contract.

Any processing of data should indicate a legal basis from the outset, in a way that is clear and sufficiently specific in order to determine what kind of processing is or is not included within the specified purpose. Any of the different conditions can be cumulative.

The Guidelines state that Article 6(1)(b) **only applies where either of two conditions is met**: the processing in question is **objectively necessary for the performance of a contract with a data subject**, or the processing is **objectively necessary in order to take pre-contractual steps at the request of a data subject**.

In order to fulfill the "objectively necessary" standard, the controller should be able to demonstrate how and why the main object of the **specific contract with the data subject cannot be performed if the specific processing of the personal data in question does not occur**. In addition, although controllers are free to design their services, if a controller wishes to bundle several separate services with different fundamental purposes into one contract, **then the applicability of Article 6(1)(b) should be separately assessed within the context of each of those services**, being mindful of what is objectively necessary to perform each of them. **This assessment may reveal that certain processing activities are unnecessary for the individual services, but rather, only necessary for the controller's wider business model**, a case in which Article 6(1)(b) would not be considered as constituting a lawful basis.

Another topic included in the Guidelines is the **retention of data after the contract is terminated**. The retention can only be lawful if controllers identify a different legal basis at the outset of processing, and communicate clearly from the commencement of the contract, as to the period during which they intend to retain records.

Finally, the applicability of Article 6(1)(b) is analysed in specific use cases, including processing for service improvement, fraud prevention and online behavioral advertising (cookies). **These use cases cannot be regarded as being necessary for a contract being entered into, as the underlying service could be provided in the absence of processing such personal data.** In such cases, controllers can rely on another legal basis/condition set out in Article 6(1).

In the case of processing for the purpose of the **personalisation of content**, the Guidelines recognise that it may, occasionally, constitute an essential or expected element of certain online services, and as such, it may be regarded as necessary for the performance of the contract. As an example, if an online news site offers a news aggregation service to users, consisting of providing users with tailored content from multiple

online sources, then it can rely on Article 6(1)(b). However, where personalised content delivery is intended to increase user engagement with a service but is not an integral part of using the service, then data controllers should consider an alternative lawful basis, where applicable.

We would be happy to provide further advice on the applicability of different legal basis for processing of personal data, according to specific details of the business and requirements.

UK Data Protection Authority Fines Company for the Illegal Collection and Sharing of Personal Data for Data Brokerage

TOPICS: Privacy, Data Brokerage, Digital Marketing, UK ICO

The UK Information Commissioner's (**"ICO"**) has imposed one of its most significant fines against the pregnancy and parenting club company Bounty, for its data brokerage activities. **The enforcement is part of a broader investigation into the data broker industry.**

Bounty provides new and expectant mothers with information and offers for products and services targeted throughout their pregnancy and beyond, collecting personal data on both the parent and children via an app, as well as offline through hard copy cards. In addition to its primary business model, the company also shares the data of its users with third parties for the purposes of electronic marketing, having disclosed more than 35 million personal data records in the course of a year to over 39 different companies, including major companies in sectors such as marketing and profiling, credit reference and telecommunications.

In analysing Bounty's practices, the ICO concluded that:

i. the data sharing was unfair as the company had failed to disclose with whom the data would be shared, particularly since its privacy policy only included a general provision indicating data sharing with third parties, without any further specification;
ii. it was not within the reasonable expectation of data subjects to have their data shared with companies in sectors such as marketing and profiling or credit reference, which could expose data subjects to potential distress without reasonable justification, other than Bounty's financial gain; and
iii. there was no appropriate legal basis for the data sharing, as consent in this case cannot be considered specific or informed, given that the subjects were not informed of the organisations with which data would be shared. The ICO also rejected "legitimate interest" as the applicable basis in this situation, given that the failure to inform data subjects of the fact of their personal data being shared with these organisations, tips the "balance of interest" against Bounty.

The ICO formed the view that Bounty's actions in sharing the data were deliberate, as it should have known that there was a risk that contravention would occur, and since it was of a kind likely to cause substantial damage or distress, Bounty had failed to take steps to prevent contravention of applicable law. The ICO also points out that in accordance with Bounty's retention policy at the time, digital records were held on an indefinite basis unless a data subject requested to be removed from the database, with children's data being retained for the duration of the parent's partnership, and was potentially shared with third parties.

In imposing the monetary penalty, the ICO took into account Bounty's financial position, the fact that the company had voluntarily ceased to disclose data to third parties and that it had subsequently made significant changes to its data practices.

FTC Settles Case Challenging Compensated Online Reviews

TOPICS: Paid Online Reviews, Digital Marketing, FTC

The Federal Trade Commission ("**FTC**") settled a case challenging a company's use of paid reviews. The complaint alleged that the company UrthBox, Inc. and its principal had **misrepresented that customer reviews were independent when, in fact, it had provided those customers with free products and other incentives to post positive reviews online.** The company also failed to appropriately disclose the terms of their "free trial" offer to consumers, which enrolled consumers in a negative option subscription plan.

UrthBox had conducted an incentive program to induce customers to post positive reviews of its snack products on the Better Business Bureau's (BBB) website, in many cases offering to send a free snack box in exchange for a positive review. As a result, the ratio of positive to negative reviews jumped from 100% negative to 88% positive, after implementation of the incentive program.

The FTC highlights that UrthBox had failed to adequately disclose that some consumers received compensation for those positive reviews, as there was no indication in the reviews that they were part of an incentive program or written in exchange for a free snack box. **According to the FTC, this practice is misleading to consumers, who should be able to legitimately assume (and trust) that reviews are impartial, and not the result of companies paying the reviewers on a clandestine basis.**

In addition, the company had failed to adequately disclose the key terms of its "free trial" automatic renewal programmes, which were offered on its websites for a nominal shipping and handling fee, including that UrthBox would charge them for six-months'-worth of shipments if they did not cancel on time. According to the FTC, a company must adequately disclose the material terms of the free trial offer before obtaining the consumer's billing information, and in addition, obtain the consumers' informed consent before charging them for the ongoing negative option subscription.

This settlement is part of the FTC's ongoing effort to combat **misleading online reviews** and is consistent with the enforcement measures taken in another recent case by the New York Attorney General, in which the practice of selling **fake followers and likes on social media** was deemed illegal, where the aim is to profit and deceive customers. It is also consistent with another recent settlement concerning a seller of fake followers and likes in social media. In this regard, our special Client Update on **influencer marketing** is relevant.

US Regulators Approach Companies Selling Cannabidiol Products based upon Unsupported Health and Efficacy Claims

TOPICS: Cannabidiol, Advertisement of Supplements, Misleading Advertising, FTC, FDA

In a joint effort, US regulators FTC and the Food and Drug Administration (**"FDA"**) sent **warning letters to three companies marketing products containing cannabidiol to treat and cure a variety of serious diseases and conditions**.

According to the letters, which the agencies sent to Nutra Pure LLC, PotNetwork Holdings, Inc. and Advanced Spine and Pain, LLC , the advertised products, ranging from oils to pills and gummies, may violate the FTC Act by making **false or unsubstantiated health claims**. Moreover, the companies' advertisements presented isolated and sparse scientific research to support claims, as well as products that can effectively treat diseases, including cancer, Alzheimer's disease, fibromyalgia, and neuropsychiatric disorders.

The FTC highlights in its letters that it is unlawful to advertise that a product can prevent, treat, or cure human disease unless the company possesses **competent and reliable scientific evidence**, including, where appropriate, well-controlled human clinical studies, which substantiate that the claims are true at the time they are made. It is also unlawful to exaggerate such claims through the use of a product name, website name, metatags, or other means, without **rigorous scientific evidence sufficient to substantiate the claims**.

In addition, the letters indicate that such claims would imply the classification of these products as drugs, since they are intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease and/or because they are intended to affect the structure or any function of the body. In any event, even if companies were to advertise the products as supplements without any scientific claims, the FDA has concluded that cannabidiol **(CBD)** products are excluded from the dietary supplement definition, since authorisation has been granted for CBD-active to be investigated as a new drug, for which substantial clinical investigations have been instituted and made public. In practice, this means that products with CBD-active should obtain prior FDA approval.

These companies have 15 days to reply to those letters, identifying specific actions taken to address the agencies' concerns in the products' advertising and dispute, and if necessary, the classification of CBD-active as a drug.

Europe Launches a Series of Regulatory Innovation Programs

TOPICS | Innovation Programs, Sandbox, Distributed Ledger Technology, AI, Privacy, ICO, EU

EU Launches International Blockchain Association to Accelerate DLT Adoption

Members of the European Commission ("**EC**"), corporations, and a wide range of blockchain startups have signed a charter to create an association the goal of which is to **promote the regulatory and business reforms needed to boost the adoption of distributed ledger technologies**.

In this context, the EC has formed the International Association of Trusted Blockchain Applications (INATBA), which is part of the European Commission effort to accelerate the adoption of blockchain technologies across a wide range of sectors. As one of its primary missions, INATBA must develop a regulatory framework concentrating on distributed ledger and blockchain technologies, by organising forums where regulators and policymakers can interact with corporations and startups to develop the necessary regulatory incentives for the technology to evolve.

Some of the main topics of attention will include **interoperability guidelines and standards**, promoting transparency, and emphasising inclusiveness.

EU Launches a Project to Pilot and Test Ethical AI Rules

As part of its ongoing efforts to develop **ethical AI rules**, the EC has announced the launch of a pilot project intended to test draft ethical rules for developing and applying artificial intelligence technologies, in order to ensure they can be implemented in practice.

This project follows the EC's High Level Group on AI publication of a draft on ethical guidelines for trustworthy AI, and aims to evaluate how the draft guidelines operate on a large-scale pilot with a wide range of stakeholders, including international organisations and companies from outside of Europe. Companies, public administrations and organisations can become members of the European AI Alliance and receive notification when the pilot starts.

On a similar topic, the Council of Europe has recently published Guidelines on Artificial Intelligence and data protection.

ICO Launches Sandbox to Support Organisations Using Personal Data

The UK's ICO is introducing a Sandbox service to **support organisations developing products and services that use personal data in innovative and safe ways**.

During this beta phase, the ICO will provide a free service for approximately ten organisations in different sectors that wish to ensure that their innovative products and services are not in breach of data protection legislation. The ICO expects that applicants will be at the cutting edge of innovation and may be operating in particularly challenging areas of data protection, where there is genuine uncertainty as to the nature and application of compliance.

UK Government Calls for the Regulation of Online Harm and Liability for Social Media

TOPICS: Social Media, Online Safety, United Kingdom

The UK Government has released a White Paper on Online Harms, the aim of which is to make the internet safer and protect vulnerable groups and particularly, children. **The Paper sets out ambitious plans for a new system of accountability and oversight for tech companies, moving beyond self-regulation**, to regulation by an **independent regulator**, which will set safety standards, supported by reporting requirements and enforcement powers.

According to the Paper, the Internet has been used to spread terrorist and other illegal, harmful or abusive content, undermining civil discourse, all of which might undermine the significant benefits, which the digital revolution can offer. While some companies have taken steps to improve safety on their platforms, the Paper states that progress has been, overall, too slow and inconsistent.

The Paper highlights that the UK Government will establish a new statutory duty of care to ensure that companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services. **Accordingly, companies will be required to ensure that they have effective and proportionate processes and governance in place in order to reduce the risk of illegal and harmful activity on their platforms**, as well as to take appropriate and proportionate action when such issues arise. The new regime will also introduce specific monitoring requirements for a specific definition of the categories of illegal content, as well as a "code of practice".

Social media firms would be required to publish annual reports on the amount of harmful content on their platforms and explain what they were doing to address this issue.

We will be monitoring this topic for future developments.

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