HFN Technology & Regulation Client Update

December 2018

Dear Clients and Friends,

2018, which is almost over, can be characterised by the numerous, significant regulatory developments the industry has seen.

We are pleased to present the latest edition of our monthly **Technology & Regulation Client Update**, which includes a variety of key regulatory, legal and industry compliance developments in the fields of personal data protection, cybersecurity; digital health, eCommerce, digital advertising and content regulations; Internet platform compliance policies; and more:

- Updated regulatory guidelines in the UK on **Data Protection Impact Assessments**;
- New Guidelines by the EDPB on the accreditation of **GDPR Compliance Certification Bodies**;
- The largest fine imposed by **COPPA in its history, on Oath**;
- Vermont's **Guidance on the new Data Broker Act**;
- FDA's detailed report on the **benefits and risks of Digital Health Tools**;
- **Fines imposed on Uber in the UK, the Netherlands and France,** following the 2016 data breach;
- **Ad-fraud enforcement actions** taken by the US DOJ and Google;
- SEC fines two celebrities for **unlawfully touting coin offerings**;
- The EU Commission's fines Guess **€40M over online sales restrictions**;
- Regulatory **Guidance in the Netherlands on Wi-Fi Tracking**; and
- ICO's fines a tax return services company for sending **14.8M spam texts**;

We would like to take this opportunity to wish our clients and friends a Happy New Year!

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

Updated Guidance on Data Protection Impact Assessments in the UK

TOPICS: Data Protection Impact Assessment, GDPR, The UK Information Commissioner's office, United Kingdom

The General Data Protection Regulation ("**GDPR**") requires organisations processing personal data, to be proactive with respect to their data-processing activities, including by continuously monitoring and evaluating their personal-data processing activities, in order to ensure that they meet the GDPR's principles and requirements. **A key requirement under the GDPR is to undergo a Data Protection Impact Assessment ("DPIA"), both as an ongoing need to assess the risks associated with their processing activities, and as the result of certain changes or events that may have occurred in the course of an organisation's life cycle.**

In addition, pursuant to the GDPR's provisions in this regard, **each of the EU member states' data protection authorities has established and published a list of the types of processing operations that are subject to the requirement of a data protection impact assessment pursuant to the GDPR. The respective lists have undergone a review by the European Data Protection Board** ("**EDPB**"), which in September 2018, issued its opinion on each list in order to harmonise the applicable regulatory approaches.

This month, the United Kingdom Information Commissioner's office ("**ICO**") **updated its Guidance on DPIA to reflect the** EDPB's opinion **with respect to the UK DPIA guidelines.**

The original version of the ICO guidance stated that a DPIA would need to be carried out where organisations plan to process biometric, genetic or location data. However, the EDPB has stated that such processing **on its own** does not necessarily represent a **high risk** and that the processing of such data **in conjunction with at least one other criterion of a "high risk" factor,** requires a DPIA to occur. The "high risk" factors are listed in the Article 29 Working Party guidance on DPIA, which was endorsed by the EDPB (see our related report here).

The updated ICO guidance reflects the EDPB's opinion, which is that the processing of biometric or genetic data will trigger the duty to carry out a DPIA only "in combination with any of the criteria in the European guidelines". The same applies to the tracking individuals' location or behaviour and in cases where the organisation plans to use innovative technology.

We would be happy to provide further advice and recommendations concerning the required DPIA process as per the GDPR.

The EDPB has Adopted Guidelines on the Accreditation of GDPR Certification Bodies

TOPICS: Certification Bodies, GDPR, European Data Protection Board, European Union

The EDPB **has adopted Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR.** According to the EDPB, the aim of the new Guidelines is to assist in the interpretation and implementation of the requirements of Article 43 GDPR, by focusing on helping member states, supervisory authorities and national accreditation bodies to establish a proper baseline for the accreditation of **certification bodies that issue certification in accordance with the GDPR**.

The key issues under the Guidelines include the following:

- **Interpretation of "accreditation" for the purpose of Article 43 of the GDPR**: The term "accreditation" is not defined under the GDPR. According to the EDPB, this term is understood as an attestation by a national accreditation body or by a supervisory authority that a certification body is qualified to carry out a certification under Article 42 and 43 GDPR, taking into account ISO/IEC 17065/2012 and additional requirements of the supervisory authority and/or the EDPB;

- **Role of member states**: Under the GDPR, member states shall ensure that although certification bodies are accredited, each member state shall determine who will be responsible for conducting the assessment prior to the accreditation. The Guidelines state that each member state should decide whether the national accreditation body or the supervisory authority will be responsible for the accreditation, while it is left to the member state to ensure that adequate resources are provided;

- **The role of the supervisory authority**: The GDPR imposes fewer obligations on a supervisory authority responsible for accrediting the certification bodies, in comparison with accreditation by national accreditation bodies. In order to maintain a harmonised approach, the EDPB states that the accreditation criteria used by the supervisory authority should be guided by ISO/IEC 17065 and in addition, complemented by the additional requirements pursuant to Article 43(1)(b); and

- **Accreditation requirements**: The Guidelines include an annex that provides **suggestions regarding the requirements, which supervisory authorities and national accreditation bodies should consider in order to ensure compliance with the GDPR**. The annex applies Article 43(2) and ISO/IEC 17065/2012 as the basis for the requirements, as well as further criteria for evaluating the data protection expertise of the certification bodies and their ability to exercise the rights of the data subjects under the GDPR. **The annex is subject to public consultation until 1 February 2019**.

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

Oath Agrees to Pay the Largest COPPA Fine in US History

TOPICS: Digital Advertising, Data Protection, COPAA, New York Attorney General, United States

Oath, known as AOL until June 2017, **has agreed to reach a settlement with the New York Attorney General** (“**the AG**”) **and pay nearly $5 million arising from charges that its online advertising business was violating the Children’s Online Privacy Protection Act** (“**COPPA**”)**.** This is the largest penalty in a COPPA enforcement matter in U.S. history.

According to the AG’s allegations, AOL conducted **billions of actions between October 2015 and February 2017 for ad space on hundreds of websites which the company knew were aimed at children under the age of 13**. In this regard, the company used cookies and geolocation information to place the ads, and disclosed this personal data to advertisers, enabling them to track and serve tracked ads to children. **By doing so, the company breached the COPPA, which prohibits websites from collecting, using or disclosing**

personal information of children under the age of 13 without obtaining prior parental consent. In addition, although AOL's policies technically prohibited the use of its display ad exchange to auction ad space on children's websites, the company knowingly did so.

Oath also agreed to adopt comprehensive reforms in its policies and procedures to protect children's privacy. Accordingly, it will establish a comprehensive COPPA compliance program, which will include the appointment of an executive or an officer to oversee this programme, annual training for relevant personnel, implementation of controls to address and monitor the relevant risks that could result in a violation occurring under COPPA, and retaining a third-party professional to assess the measures taken by the company. Moreover, AOL will destroy all personal information in its possession, custody or control previously collected from minors.

Vermont AG has Published Guidance on New Data Broker Regulation

TOPICS: Data Protection, Data Brokers, Vermont, United States

The Vermont Attorney General's Office has issued a guidance in order to **assist data brokers in complying with Vermont's new Data Brokers Act** (Act 171 of 2018) ("**the Act**").

The Act **takes effect on 1 January 2019** and, among other things, requires "**data brokers**" to register with the Vermont Secretary of State and to protect the personal information of Vermont residents (for more information about the Act see our related update here, and our special update regarding the legislative developments in US privacy and data security here).

The Guidance explains the definitions of key statutory terms and the scope of the regulation, and includes the following clarifications:

- **In order to determine whether a business shall be considered a data broker** under the Act, the Guidance suggests that the following considerations be taken into account:
  a. Is there a direct relationship between the business and the consumers?
  b. Does the business both collect and sell or licence the personal data?
  c. Does the data concern Vermont residents?
  d. Is the data considered "brokered personal information" as defined in 9 V.S.A. § 2430(1)?

- **Registration**: The Guidance includes a copy of the annual filing form, and addresses several questions on how to fill in the form. For example, it explains that under the section regarding the implementation of a purchaser-credentialling process by the data broker, the term credentialling refers to the practice of taking reasonable steps to verify the identity of the data broker's customers, and that this process is considered "best practice" under the regulation.

- **Data security standards**: The Guidance specifies **the minimum data security standards** under the regulation. Such standards include the following:
  a. Development, implementation and maintenance of a comprehensive security program;
  b. Designating at least one employee to maintain the program;
  c. Performing a risk-assessment procedure;

d. Employee training;
e. The data broker shall supervise service providers; and
f. The data broker shall have the means for detecting and preventing security system failures.

We would be glad to advise our clients and clarify the implications arising from Vermont's Data Broker Act and the new Guidance.

The FDA has Published a Report on the Benefits and Risks of Digital Health Tools

TOPICS: Digital Health Compliance, Patient Safety, FDA, United States

The US Food and Drug Administration ("**FDA**") has **released a new report on "non-device software functions: impact to health and best practices". The report includes the FDA's analysis of the potential benefits and risks of software products not regulated by the FDA, such as medical devices, e-prescribing software or mindfulness apps.**

The report is based on information published in relation to the US population during the last two years, and will be published biennially, **focusing on five types of software functions**, as required by Congress:

- administrative support of a healthcare facility;
- products that encourage a healthy lifestyle, such as mindfulness apps;
- certain types of electronic patient records;
- specific types of software that transfer, store or display clinical laboratory tests or other device data and results; and
- certain types of clinical decision support software, such as those that identify drug interactions.

The majority of the findings in relation to the five software functions in this report are positive, and demonstrate that they have a positive impact on their users' safety and health, with minimal negative impact reported.

Some of the best practices according to the report include the following:

- **For products that encourage or maintain a healthy lifestyle** - recommendation to notify users as to the difference between a health product and a medical device;

- **For electronic patient records software** - recommendation that patient education information and care-plan details be included in the electronic health record ("EHR") portal, since this will enable them to be more engaged and informed with respect to their treatment. In addition, it is important that all stakeholders that view the EHRs will be engaged in the software's development, verification and validation, since it is likely that the developers will not have the required clinical understanding. Moreover, in order for the patients to be able to understand their health data and recommendations, it is important to design the user interface accordingly;

- **For software that transfers, stores or displays clinical laboratory tests or other device data and results** - recommendation that a software overlay be used to collect data from databases (extract), format the

data and information in a uniform language (transform), and then transfer or insert the data and information into the targeted software (load). This type of method allows the data to be merged;

- **For certain types of clinical decision support software** - it is suggested that their design should make it possible for doctors to use clinical intuition and to work around the alerts. It is also recommended that if an alert is ignored, documentation as to the rationale should be required; and

- **For administrative support of a health care facility software -** it is recommended that in order to prevent errors in patients' information, character fields should be sufficiently long (approximately 50 characters).

The FDA stated that while they believe the such products give rise to more benefits than risks to patients, they nevertheless recommend that consumers and healthcare providers who use these technologies, should **be informed as the advantages and disadvantages of these and any digital health products they are considering using or recommending to their patients**.

Uber Fined by 3 EU Watchdogs in excess of $1.6M Resulting from a 2016 Data Breach

TOPICS: Data Protection, Data Breach, Data Protection Authorities, United Kingdom, The Netherlands, French

The ICO, the Dutch Data Protection Authority ("**Dutch DPA**") and the French Data Protection Authority (the "**CNIL**") **collectively fined Uber more than $1.6 million for failing to protect customers' personal information during a 2016 cyber-attack, which involved millions of users** (Uber Technologies, Inc. was already fined by the Attorney Generals in all 50 US states in late September; see our related update here**).**

The ICO fined Uber more than $490,000 due to several avoidable data security flaws which affected approximately 2.7 million UK customers, and the Dutch DPA imposed a $678,000 fine on Uber for not reporting the data breach, which affected 174,000 Dutch citizens, within 72 hours. The CNIL fined Uber $460,000, given that the data breach affected 1.4 million users in France. All fines were imposed under these states' respective pre-GDPR legislation.

According to the ICO, their investigation disclosed several avoidable data security flaws that allowed the personal details of the company's customers to be accessed and copied from an Amazon cloud-based storage system, operated by Uber US, that served as the data processor of the personal information. The attackers used '**credential stuffing**' - a process by which the compromised username and password pairs are injected into a website until they are matched to an existing account.

The ICO stated that **the security arrangements adopted by Uber US were inadequate**: its policies did not properly cover the risks presented by the use of third-party platforms, such as GitHub, without having multifactor authentication in place, where the repository includes an access key in plaintext. In addition, the account credential in the service account was contained in plaintext in a piece of code that was stored in GitHub. Furthermore, according to the ICO, **Uber US's decision to treat the incident as a "bug bounty" rather than a security breach, reflects the company's inadequate decision-making**.

The ICO considered Uber contraventions as serious in light of the large amount of the personal data and the fact that the attack was neither reported to the ICO (or any other relevant regulator), nor to the individuals whose personal data had been compromised at the time.

The ICO took into account other mitigating circumstances, such as the fact that the local branches of Uber were not aware of the security breach at the time and therefore were not in a position to report it; the fact that there is no evidence that the personal data was successfully used for identity theft or fraud; and the fact that substantial and prompt remedial actions had been taken.

The CNIL, which fined the company several weeks after the ICO and the Dutch DPA had imposed their fines, also argued that the data breach could have been prevented by implementing certain elementary security measures, and practically invoking the same measures stated by the ICO.

DOJ and Google Fight Ad Fraud Schemes

TOPICS: Digital Advertising, Adtech Industry Compliance, Google Play, Department of Justice, United States

DOJ has Charged Eight People in Massive Online Ad Frauds

The US Department of Justice ("**DOJ**") **has charged eight men from Russia and Kazakhstan with running multimillion-dollar online ad fraud**. According to the allegations, as a result of the fraud schemes the defendants managed to collect a total of **more than $36 million from companies which believed they were paying for ad views, while the ads were never actually seen by humans, according to the indictment**.

According to the DOJ's announcement, the defendants are accused of running two separate, but related, fraud schemes: the first is Methbot, a datacentre-based scheme that used more than **1,900 rented computer servers** to load ads on fabricated websites and created an illusion that real users were viewing the ads. The second fraud scheme, 3ve, was based on a **global botnet network of more than 1.7 million malware-infected computers**. The defendants sent commands to those computers to download fabricated webpages and load ads into them, thereby falsifying billions of ad views.

The charges against the defendants include **wire fraud, money laundering, computer intrusion and aggravated identity theft**. The US State Attorney stated that this case demonstrates the efforts invested by the US Attorney Office and its law enforcement partners in order to fight against these costly fraudulent schemes.

Google Removes Popular Android Apps Over Ad Fraud

Google announced that it has conducted an investigation after the company received reports of apps on Google Play which were conducting app install attribution abuse. **The apps were used to falsely claim credit for newly installed apps in order to collect the advertising download-based fee from that app's developer**.

During the investigation, Google removed two popular apps from its Play Store and made this enforcement step public by naming CM File Manager and Kika Keyboard, for app install attribution abuse. **In addition, Google discovered three malicious SDKs that were being used to conduct ad fraud.** The company believes

that some of the app developers using these SDKs were unaware of the ad fraud scheme, and granted them a grace period in order to take action.

The CM File Manager has published that it takes this issue very seriously and is in continuous communication with Google Play in order to resolve this matter**. Google added that it continues to investigate in order to protect against abusive behaviour and provide users with safe and secure experiences**.

The SEC Fines Two Celebrities for Unlawfully Touting Coin Offerings

TOPICS: Social Influencers, Initial Coin Offering, SEC, United States

The US Securities and Exchange Commission ("**SEC**") **announced it has charged two celebrities: DJ Khaled and pro boxer Floyd Mayweather Jr., for failing to disclose the fact that they were being paid promotional fees in order to promote initial coin offerings** ("**ICOs**").

These cases come after the SEC issued **a warning** in November 2017 **to celebrities and social influencers who promote ICOs, that they must disclose the nature, source and amount of any payment they receive for such promotion** (in this regard you can see our special Client Update concerning influencer marketing). This is the first time the SEC has issued charges for touting violations involving ICOs.

According to the SEC, the cases demonstrate the importance of full disclosure to investors. However, the SEC stated that the investors should not make decisions based on celebrities or social media influencer promotions, as they often receive payment for such endorsements.

Both celebrities agreed to pay settlements, which included penalties and interest: Mayweather agreed to pay a total of $614,755, and Khaled agreed to a payment of $152,725. Additionally, the celebrities agreed to avoid the promotion of any kind of securities for three and two years, respectively.

The EU Commission Fines Guess €40M over Online Sales Restrictions

TOPICS: e-Commerce, Geo-blocking, Competition Law, Guess, European Commission, European Union

The European Commission ("**the EC**") announced that it has imposed an antitrust **fine of almost €40 million on the Guess clothing company for illegally prohibiting retailers from using its brand names and trademarks for the purpose of online search advertising and making cross-border sales of Guess products**. The fine was reduced by 50 percent due to the company's cooperation during the investigation.

The EEA competition rules state that consumers must be free to purchase from any retailer authorised by the manufacturer, and that these manufacturers should be able to offer the products online, as well as to advertise them and sell them on a cross-border basis. However, according to the EC, the objective of Guess' distribution agreements was to prevent EU consumers from shopping in other member states by **restricting retailers from advertising and selling cross-border without obtaining Guess' prior consent**. As a result, the company could maintain higher retail prices. This illegal practice, according to the EC, has a negative impact

on competition and cross-border trade and consequently, damages the functioning by the Commission of the EU's Digital Single Market strategy.

The EC's decision **complements Regulation 2018/302 on unjustified geo-blocking** (for more information regarding this Regulation, see our related update here). The Regulation prohibits, in some situations, a supplier from contractually prohibiting the retailer from responding to unsolicited customer request, which is also known as "passive sales". In addition, the Regulation allows restrictions on "active sales" (i.e. actively approaching and targeting customers) where those restrictions comply with the EU competition rules, unlike in this particular case.

London Company Fined for Sending 14.8 Spam Texts

TOPICS: Direct Marketing, Consumers' Protection, PECR, The ICO, United Kingdom

The ICO announced it has fined **tax return company, Tax Returned, £200,000 for sending 14.8 million spam SMSs without obtaining the users' consent, using a third party service provider**. The ICO investigation found that the company violated Regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**"), which bans the transition of unsolicited communications for the purpose of direct marketing by means of electronic mail, including any text, voice, sound or image message, unless the conditions stated in Regulation 22 are met.

The ICO found that a total of 2,146 complaints were made by individuals who received the communication but did not provide their consent to receiving such marketing communication. According to the ICO, the wording of the company's policies were insufficiently clear and neither Tax Returned nor the third party service provider were listed on most of those privacy policies. Accordingly, millions of text messages had been sent in the absence of valid consent.

The ICO added that in the past, Tax Returned had **received an enforcement notice from the ICO** that ordered the company to cease its illegal practice and ensure they had obtained all necessary consent, even when using third-party marketing services, which it promptly ignored.

Dutch DPA Releases Guidance on Wi-Fi Tracking

TOPICS: Data Protection, Wi-Fi tracking, GDPR, Dutch DPA, The Netherlands

The Dutch DPA has released a new **Guidance as to when companies can track individuals using Wi-Fi.** This publication follows the CNIL's publication of new rules regarding audience and traffic measuring in publicly-accessible areas last month (see our previous update here).

According to the Guidance, companies are only allowed to follow people via Wi-Fi tracking in exceptional circumstances. In this regard, the Guidance states that **companies can track individuals only based on three legal grounds**:

- where they have obtained the individual's consent;
- where a legitimate interest exists on their part; or
- for the purpose of executing an agreement.

Even so, the company will have to consider if there are less intrusive alternatives, and use Wi-Fi tracking only when necessary. The Dutch DPA added that the processing of such data must comply with the GDPR.

In addition, the Dutch DPA has published a detailed explanation in the form of a Q&A. It explains that organisations that are not private companies, such as municipalities, may process personal data via Wi-Fi tracking and Bluetooth tracking **only in precisely defined areas, only where this is strictly necessary, and for a limited duration**. It also explains that when a company bases the tracking on the individual's consent, such **consent must comply with the GDPR's standards, and consequently, it might become complicated on a technical basis**.