HFN Technology & Regulation Client Update

January 2019

Dear Clients and Friends,

We are pleased to present the latest edition of our monthly **Technology & Regulation Client Update**, which includes, amongst others, a variety of notable regulatory and industry compliance developments in the fields of personal data protection, cybersecurity, digital advertising and content regulations, as well as Internet platform compliance policies. These include the following:

- **Brazil creates a data protection authority**, following the approval of its new **data protection law**;
- The Austrian privacy regulator permits the establishment of a **paid subscription model under the GDPR**;
- The European Commission adopts **an adequacy decision on Japan**;
- The French privacy regulator imposes a **€50 million fine on Google** and publishes **guidance on sharing personal data** with business partners;
- The US health regulator issues **cybersecurity guidance for the healthcare sector**; and
- The State of Massachusetts **amends its data breach reporting laws, creating additional requirements**.

Kind regards,

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

Brazil Creates a Data Protection Authority Following the Approval of Data Protection Law

TOPICS: Data Protection, Brazil's General Data Protection Law

Following the enactment of Brazil's new Data Protection Law ("LGPD"), originally set to become effective in February 2020 and now delayed until August 2020, Brazil's former President issued an Executive Order (MP 869/18) creating Brazil's Data Protection Authority.

The Authority will consist, at the highest level, of five commissioners, to be appointed by the Brazilian President, having three primary functions:

(i) rulemaking and **interpretive guidance**;
(ii) **investigation and enforcement**; and
(iii) **education**.

In order to provide support to the Authority, the **National Council for the Protection of Personal Data** was also established, composed of representatives from government, private industry, academia and civil society.

Once the new Authority commences operation, it is expected to issue a set of clarifications regarding the details of the LGPD, including the meaning of "legitimate interest", the legality of certain international data transfer mechanisms, acceptable anonymisation techniques and the scope as to the application of the law.

We will continue to track developments relating to data protection and cybersecurity in Brazil and Latin America in general, a region in which privacy and cyber laws are beginning to gain traction, creating new challenges as well as exciting opportunities.

Austrian Privacy Regulator Permits Paid Subscription Model

TOPICS: Data Protection, Ad-tracking, GDPR, Austrian Data Protection Authority, European Union

The Austrian Data Protection Authority ("**DSB**") **has published a decision in response to a complaint from an individual against an online media publisher, regarding its cookie consent practice**. The media publisher offered three options to individuals wishing to access the content on its website:

(i) to consent to advertising cookies and have full access to the website;
(ii) to refuse cookies and receive a limited access to the website; or
(iii) to refuse cookies and receive a full access to the site via an online subscription, the cost of which is €6 per month. The complainant argued that this website did not meet the requirements for **freely given consent** under the General Data Protection Regulation (the "**GDPR**").

The DSB dismissed the complaint and held that this practice met the conditions for consent under the GDPR. The DSB noted that **online media companies usually rely on advertising as the only source of revenue and consequently, the requirement of freely-given consent could not oblige media companies to provide their services free of charge**. The DSB also noted that the publisher had developed a privacy-conscious product that offered a pay-for-subscription or tracking-free option for users and thus provided different options.

In its decision, the DSB referred to the Article 29 Working Party Guidelines on Consent (which have been endorsed by the new European data protection regulatory body - the European Data Protection Board), according to which, consent will be deemed as not freely given if there is a risk of deception, intimidation, coercion or significant, negative consequences in the event of the individual not providing his/her consent. **The DSB found that the price of €6 per month was not a disproportionately expensive alternative, and in any case, users have the option to choose another online publisher.**

This decision might be seen as an indication that media companies, especially online media companies which rely on advertising as the only or main source of revenue, have **legitimate business interests in ad tracking**. However, this decision does conflict with the UK's Information Commissioner's Office ("**ICO**") approach: **in a similar case** involving the Washington Post website, **the ICO held that since the Washington Post did not offer a free alternative to accepting cookies, consent cannot be freely given**.

We would be happy to advise our clients with respect to the practical implications of these regulatory decisions with respect to privacy aspects in online advertising and publishing.

European Commission Adopts Adequacy Decision on Japan - Allowing the Flow of Personal Data Between Countries

TOPICS: Data Protection, Adequacy Decision, GDPR, Japanese Act on the Protection of Personal Information, European Union

The European Commission ("EC") has adopted an adequacy decision on Japan, allowing personal data to flow freely between these two significant regions, resulting in the creation of the world's largest area of safe data flows, benefitting the economies of both the EC as well as Japan. In this regard, the adequacy decision also complements the EU-Japan Economic Partnership Agreement, which will enter into force in February 2019.

An adequacy decision is a decision taken by the EC, pursuant to the GDPR, establishing that a third country provides a **comparable level of protection of personal data to that which prevails in the European Union, under its domestic law or international commitments**. So far, the EC has adopted adequacy decisions for Andorra, Argentina, Canada, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland and Uruguay, as well as partial adequacy decisions for the United States (limited to the EU-U.S. Privacy Shield framework).

Japan has recently modernised its data protection law applicable to the private sector, by enacting the Japanese Law on the Protection of Personal Information, bringing it closer to the European standards. Following the negotiations with the EC, **the Japanese Government has adopted Supplementary Rules applicable only to data transferred from the EU**, thereby closing the remaining gaps. These supplementary rules expand the Japanese definition of "sensitive data", the exercise of individual rights by European citizens, and the conditions under which EU data can be transferred from Japan to another third country.

European citizens will also be granted various possibilities of obtaining redress concerning their personal data in Japan, including filing a complaint to the Japanese Data Protection Authority, recourse to mediation, or by filing a civil action to the Japanese courts for damages or an injunction.

The Japanese government has also given assurances to the EC regarding the use of data **for criminal law enforcement and national security purposes**, such that any such use of personal data would be limited to what is necessary and proportionate and be subject to independent oversight and effective redress mechanisms.

French Privacy Regulator Imposes a 50 Million Euros Fine against Google

TOPICS: Data Protection, Ad Personalisation, GDPR, The French National Data Protection Commission, European Union

In a historical first, the French National Data Protection Commission's ("**CNIL**") restricted committee **applied the new sanction limits provided by the GDPR,** imposing a **financial penalty of 50 Million Euros against Google**.

The CNIL initiated its investigation after receiving a number of complaints alleging that Google had no valid legal basis to process the personal data of the users of its services, particularly of Android users that had opened a Google account, for **ad personalisation purposes**, and concluded that Google did not comply with the GDPR's provisions.

An initial key outcome of this investigation relates to the CNIL's competence in assessing and determining this matter. Although the GDPR establishes a "one-stop-shop mechanism", which provides that an organisation established in the European Union shall have only one main regulator, namely, the Data Protection Authority of the country where its "main establishment" is located. **In this particular case, it was determined that Google had no main establishment in Europe**. As such, even though Google has headquarters in Ireland, the Irish establishment did not have a decision-making power on the processing operations carried out in the context of the Android operating system and the services related to the creation of an account during the configuration of a mobile phone. Accordingly, the CNIL found that together with other EU regulators, it was competent to investigate this matter and to take enforcement measures against Google.

With respect to the material issue investigated in this matter, the CNIL found that there had been **two distinct breaches of the GDPR:**

- **Insufficient transparency and information** - according to the CNIL, Google had violated its obligation to provide transparency and information for the following reasons:
  - (i) relevant information on data processing is only accessible by the user after various steps had been taken, including demanding 5 to 6 different actions, such as when the user wishes to collect information on how his/her data is used for ad-personalisation or geo-tracking;
  - (ii) the objective of processing is described in a generic and vague manner, as are the categories of data used for different purposes;
  - (iii) information regarding ad-personalisation is not communicated to users clearly enough in order to be understood as having a legal basis of consent, rather than concentrating on the company's legitimate interest; and
  - (iv) the data storage periods, or the categories of personal data used for the ad-personalisation, are excessively disseminated across several documents, with buttons and links that users are required to click in order to access complementary information.

- **Invalid Consent** - the CNIL found that Google's consent flow does not comply with the GDPR, based on the following reasons:
  - (i) consent is not sufficiently informed;
  - (ii) information regarding the processing of data for ad-personalisation is diluted in different sources and does not allow users to be easily aware of its extension;
  - (iii) it is not possible to fully understand the plurality of services, websites and apps involved in the processing activities (Google search, YouTube, Google Home, PlayStore, etc.), and accordingly, the quantity of processed data combined from different sources for ad-personalisation renders the consent non-specific or equivocal;
  - (iv) the display of consent for ad-personalisation is pre-ticked, while consent is "unambiguous", according to the GDPR, which requires a clear affirmative action from the user (by ticking an empty box, for instance); and
  - (v) before creating an account, the user is asked to generally consent to "*the processing of my information as described above and further explained in the Privacy Policy"* in order to create the account, giving a consent in full for all Google activities, while the GDPR requires consent to be specific.

According to the CNIL, the amount and the publicity of the fine are justified by the severity of the infringements observed, which are contrary to the essential principles of the GDPR: transparency, information and consent. Other factors taken into consideration are the continuous nature of the breach (not a one-off, time-limited infringement), the presence that the Android operating system has on the French Market, with thousands of people creating a Google account from their smartphone every day, and the company's business model, which is partly-based on ad-personalisation.

Google is set to appeal against this decision. However, the decision itself is a strong and robust indicator that companies, which combine data for ad personalisation, need to exercise significant care with respect to the lawful ground of processing under the GDPR, as well as with all the various aspects of obtaining informed consent, when required.

We would be happy to assist our clients in understanding and addressing the strategic and practical consequences of this decision.

US Health Regulator Issues Cybersecurity Guidance for Healthcare Sector

TOPICS: Cybersecurity, Healthcare, US Department of Health & Human Services

In a demonstration of the high priority being given to cybersecurity in healthcare services, the US Department of Health & Human Services ("HHS") has issued guidance on cybersecurity for healthcare organisations. The report is the result of a task group created by the Cybersecurity Act of 2015 and comprised of more than 150 healthcare and cybersecurity experts.

The document **examines current cybersecurity threats affecting the sector**, identifies **specific weaknesses** that make organisations more vulnerable to the threats, and provides **selected practices** which cybersecurity experts rank as the most effective in order to mitigate those threats.

HHS emphasises that vulnerabilities constitute weaknesses within an organisation which could be harmful or even devastating if breached. According to the report, **the most current and common cybersecurity threats to healthcare organisations are**:

(i) e-mail phishing attacks;
(ii) ransomware attacks;
(iii) loss or theft of equipment or data;
(iv) insider, accidental or intentional data loss; and
(v) attacks against connected medical devices that may affect patients' safety.

In addition to the main report, which is deliberately written in plain language in order to raise awareness, HHS also provides two **technical volumes** that contain implementation recommendations for ten cybersecurity practices, focused on IT and IT security professionals. It also recognises that healthcare organisations require current and resilient cybersecurity that is compatible with their needs, **without restricting innovative efforts relating to the areas of the population's health, precision medicine, and transparency.**

Use of the document is not mandatory and is neither required nor guarantees compliance with relevant laws, but rather, intends to provide voluntary, consensus-based principles and practices in order to improve cybersecurity in the health sector. The guide also expressly refrains from a "one size fits all" approach, by recognising that **it is critical to tailor cybersecurity practices to a healthcare organisation's size.** To emphasise this variation, the technical volumes separately set out cybersecurity practice implementations for small, medium-sized, and large organisations.

However, the report cautions, that identifying the size of an organisation is not as simple as it may seem, and accordingly, provides a table to guide organisations in their evaluation, as well as an evaluation methodology and toolkit to offer guidance on implementation, according to risk assessment and specific needs.

We would be happy to provide advice and recommendations, concerning the technical implementation of the guidelines, and in helping companies assess their cybersecurity threats and needs, by performing a risk assessment report and benchmarking best practices.

French Privacy Regulator Publishes Guidance on Sharing Personal Data with Business Partners and Other Third Parties

TOPICS: Data Protection, GDPR, The French National Data Protection Commission, European Union

The CNIL has published guidance regarding the compliance conditions in order for organisations to **lawfully share personal data with business partners or other third parties**, such as **data brokers**, within the context of the GDPR.

The guidance focuses on five key requirements:

(i) **Prior consent, which must be freely given, specific, informed and unambiguous, according to the GDPR standards**. In addition, the partners may not share the personal data with their own partners, without obtaining the individual's consent;

(ii) **The organisation that first collects the data must complete the data collection form with either an exhaustive and updated list of** partners, or insert a link to that list in the form, together with a link to the partners' privacy policies;

(iii) **Inform individuals of any updates to the list of partners and the fact that their personal data may be shared with new partners**, ensuring that each marketing message sent by the organisation that collects the data, sets out an up-to-date list of partners. In addition, each new partner receiving data must inform the individual, in the first communication to the data subject, of the processing of data;

(iv) **The partners who process personal data in order to send marketing communications, must inform the concerned individuals of the source from which the data originates** (by providing the name of the organisation who shared the data with them), and how individuals may exercise their **data protection rights**; and

(v) The guidance emphasises the right of individuals to object to the use of their data, either directly by contacting the partner, or by contacting the organisation who first collected the data. In the latter case, the organisation is required to pass on the objection to the partner.

The State of Massachusetts Amends Data Breach Reporting Laws, Creating Additional Requirements

TOPICS: Data Breach, Credit Monitoring Services, Massachusetts, United States

The State of Massachusetts has approved the Act on Consumer Protection from Security Breaches, which amends its current data breach reporting law, creating additional requirements on certain aspects such as the timing and the content of data breach notifications.

The new Act also requires organisations to **provide credit-monitoring services** when social security numbers may have been compromised as a result of the breach (for more information regarding the **new privacy legislation of certain States, see our special update here**).

Under the Massachusetts data security laws, any entity that owns or licences personal information regarding a Massachusetts resident, is currently required to develop, implement, and maintain a **comprehensive written information security program**. This also includes provisions for responding to data breach.

With this amendment, **entering into force on 11 April 2019, additional required information for the breach notice** now includes providing information such as: the name and address of the person that experienced the breach of security, the person responsible for the breach, if known, and the type of personal information compromised, as well as the resident's right to obtain a police report and request a security freeze without charge. Entities are also required to submit to the regulators, a sample of the notification letters that they send to consumers. If the company experiencing a breach is owned by a separate entity, then the individual's notice letter must specify "the name of the parent or affiliated corporation."

As to the timing of the notice: this must be issued as soon as possible, and **affected entities may not delay on the grounds that the total number of individuals** affected has not been determined, but rather, additional notices should be sent as soon as practicable on a rolling basis.

Finally, if there is a possibility that social security numbers have also been affected, then **entities must "contract with a third party to provide" free credit monitoring services** to the impacted Massachusetts residents, at no cost, for a period of at least 18 months (42 months, if the company is a consumer reporting agency).

We would be glad to advise our clients and clarify the far-reaching implications arising from the new US privacy legislation developments.

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