HFN Technology & Regulation Client Update

November 2018

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 new EU regulatory Guidelines on the **territorial scope of the GDPR**;
- Various industry and regulatory measures in the area of **influence marketing regulations** and **integrity in social media platforms**;
- New regulatory rules in the UK on the **use of personal data for marketing** and guidance on **encryption and passwords** under the GDPR;
- The UK Government's and competition and financial regulators' review of **personalised pricing practices**;
- **GDPR enforcement actions against online advertising company** and **regulatory guidelines on audience and traffic measuring** by the French data protection authority;
- Intel's proposed **Federal US privacy law**;
- The Israeli National Cyber Directorate's recommendations on **organisations' readiness for cyber crisis and IR teams**;
- The Israeli Banking Supervision Department's **regulatory changes concerning the use of cloud computing technologies** and a **mandatory Board of Directors Committee for Technology and Innovation**;
- Google Chrome's new measures against **ads from abusive sites**; and
- The Dutch governmental audit's findings concerning **Microsoft Office's data collection practices**.

Kind regards,

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

Guidelines Published by the EU Data Protection Regulator on the Territorial Scope of the GDPR

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

The European Data Protection Board ("**EDPB**") has published its long awaited **Guidelines on the GDPR's Territorial Scope** ("**the Guidelines**") for public comment. The aim of the Guidelines is to clarify a number of open questions concerning the **territorial scope of the General Data Protection Regulation ("GDPR"), and in particular, where the data controller or processor is established outside of the EU.**

According to Article 3 of the GDPR, its provisions apply to:

- An **EU-based controller or processor** processing personal data in the context of its activities; or
- A **non-EU based controller or processor** processing **personal data of data subjects in the EU** in connection with either the **offering of goods or services**; or **the monitoring of their behaviour** taking place in the EU.

The Guidelines provide clarification for companies to assess whether all or parts of their activities will fall under the scope of the GDPR and, if so, to what extent they would be subject to the application of the GDPR. Notably, the Guidelines provide clarifications on a number of subjects that have been viewed as controversial since the enactment of the GDPR, including the following:

- Application of the GDPR to the establishment of a controller or a processor in the Union "regardless of whether the processing takes place in the Union or not". In this regard, the EDPB states that any personal data-processing in the context of the activities of an establishment of a controller or processor in the Union, would fall under the scope of the GDPR. In order to determine whether a non-EU entity has an establishment in the EU for the purpose of the GDPR, both the degree of stability of the arrangements and the effective exercise of activities in that Member State must be considered, in light of the specific nature of the economic activities of the services;
- A non-EU controller using an EU processor for activities outside of the EU, which does not target EU residents, is not required to comply with the GDPR. The EU processor will be subject to the relevant GDPR provisions that are directly applicable to data processors;
- Citizenship, established residency or any other type of legal status of the data subject, is irrelevant when determining the application of the targeting criteria; and
- The criteria of the appointment of an EU representative is in accordance with Article 27 of the GDPR for non-EU controllers and processors.

The Guidelines will still be subject to public comment prior to ratification.

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

Regulators and Industry Fight for Integrity on Social Media Platforms

TOPICS: Influencer Marketing, Consumer Protection, The Securities and Exchange Commission, Federal Trade Commission, Instagram, United States

The FTC Settles with PR Firm and Publisher over Undisclosed Sponsored Posts

The FTC has published that it has settled with two Georgia-based companies and their principals with regard to allegations of their having **misrepresented product endorsements as independent opinions, and commercial advertising as editorial content** (you can read more about influencer-marketing in our special client update titled "Influencer Marketing - Rules of Engagement").

According to the FTC's complaint, Creaxion Corporation ("**Creaxion**"), a marketing and public relations company, and its CEO, were hired by HealthPro Brands Inc. ("**HealthPro**") to help in the launch and promotion of an organic mosquito repellent. Creaxion collaborated with Inside Publications, the publisher of Inside Gymnastics magazine, in order to obtain athletes to endorse and otherwise promote the product. Subsequently, Creaxion and Inside Publications **engaged two Olympic gold medalists as endorsers, who each received several thousand dollars for their promotional activities, which included social media posts of the product.**

According to the FTC's allegations, **in numerous instances, the endorsements did not disclose the spokespersons' paid promotional relationships with HealthPro**. In addition, Inside Publications reposted those statements on social media, without such disclosure being made. Inside Gymnastics also ran paid ads for the products that were disguised as features or other articles of interest to its readers. **In addition, according to the complaint, Creaxion reimbursed employees and "friends" for buying the product and posting positive reviews.**

As a result, FTC's complaint alleges that the respondents **violated the FTC Act by**: (i) falsely representing that the endorsement represented their independent opinions; (ii) failing to disclose material connections between the endorsers and the marketer, specifically, that they were paid or reimbursed for the publications; and (iii) falsely representing that paid ads were independent statements and opinions.

The proposed settlements prohibit:

a) misrepresentations regarding the status of any endorser or reviewer;

b) making any representation as to any consumer or other endorser of such product or service without clearly disclosing any unexpected material connection between the endorser and any respondent, or other individual or entity affiliated with the product or service; and

c) any misrepresentation that paid commercial advertising constitutes a statement or opinion from an independent or objective publisher or other source. In addition, the proposed settlements require the respondents to take steps to monitor endorsers acting on their behalf.

Instagram Fights Inauthentic Activities

Instagram announced that it is taking several steps in order to reduce inauthentic and fraudulent behaviour. In this regard, Instagram disclosed that some accounts have been using third-party software in

order to artificially increase their audience. These tactics harm the real and genuine experience that users seek, and also renders these accounts less secure. **Accordingly, Instagram stated it would begin to remove inauthentic 'likes', follows and comments from accounts that use third-party apps in order to boost their popularity, and using a machine-learning tool that the company has built, which is able to identify accounts that use such services.**

Accounts identified as inauthentic will receive an in-app message alerting them to the fact that Instagram has deleted the unauthentic content. In addition, Instagram will advise users, who may have unintentionally used third-party services such as these, to secure their account by changing their password. Instagram added that it will continue to monitor these kinds of activity in the future, and that it is about to publish more updates on additional measures taken by the company in order to remove inauthentic activity on its platform.

SEC Charges Giga Entertainment Media and Several Former Offices and Directors with Fraud in Connection with an Advertising Scheme to Mislead Investors

The US Securities and Exchange Commission ("SEC") announced it has filed **a complaint against social media technology company, Giga Entertainment Media** ("**Giga**"), **and five previous officers and directors of the company for deceiving investors regarding the company's Apple Store download ranking**, and faking documents to cover up the fact that one of its officers has a criminal record.

According to the complaint, during 2016 Giga acquired more than 559,600 downloads from outside marketing firms in order to boost the profile of the company's mobile app. **Consequently, Giga received "a shortcut" to boost its app among Apple Store download standings, while it misled its investors into believing that the high ranking is the outcome of a successful advertising.**

Furthermore, when the company ceased to pay for the app's downloads, resulting in a significant decrease in its downloads, the company and its stakeholders fraudulently informed investors that the number of downloads continued to increase at the same rate. Additionally, the SEC alleges that Giga's stakeholders were also dishonest and distorted documents, such that the investors would not know of the company's "de facto CEO" previous criminal charges of mail fraud.

The SEC stated that this complaint should remind companies that they cannot "buy their own crowd" and then claim to be popular, but rather, they must be honest with investors. According to the SEC, the former Giga offices pleaded guilty to violating antifraud and securities laws. Two of them will each pay $25,000 in penalties and a third officer will pay $15,000, with several others agreeing to a five-year bar, and the court will later determine the penalty applicable to the other stakeholders.

The CAP Announces New Rules on the Use of Personal Data for Marketing

TOPICS: Digital Advertising, Data Protection, Committee of Advertising Practice, United Kingdom

The UK's Committee of Advertising Practice ("CAP") has announced an amendment to the UK Advertising Code ("CAP Code"), to include new rules on the use of data for marketing. The new rules, which take immediate effect, have been introduced following public consultation in order to ensure that they cover data protection issues most relevant to marketing and that they are aligned with the GDPR standards.

The amendments relate to Section 10 of the CAP Code, which regulates **the use of data for direct marketing**, and to Appendix 3, which includes rules on **transparency and the control** of data collected, which is used for the purpose of delivering adverts according to the users' browsing behaviour.

The key changes to the CAP Code are:

- The amendment added and revised several definitions in section 10, such as the definition of consent, personal data, special categories of personal data and controllers.

- The amendment added, inter alia, the following rules under section 10:
  - Marketers must not make persistent and unwanted marketing communications by telephone, fax, e-mail, or other remote media;
  - When collecting consumers' personal data, marketers must provide consumers with some information, such as the identity and contact details of the marketer, the purposes and legal basis for the collection and the recipients or categories of recipients of the personal data;
  - Where marketers intend to further process personal data for a purpose other than initially intended, they must ensure the new purpose is compatible with the original purpose and provide consumers with information, such as by further privacy notice; and
  - Marketers must obtain prior consent from consumers before processing their personal data in order to send marketing communication, or be able to demonstrate that the processing is necessary for the purpose of their, or a third party's, legitimate interest. Said legitimate interest may not override fundamental rights and freedoms of the consumers.

- The amendment has removed the rules regarding data security and transfer outside of the European Economic Area (EEA), access to data, persistent and unwanted marketing communication, publicly available information and the nature of personal information and retention from Section 10.

- The amendment has also removed Appendix 3, which was related to online behavioural advertising, as this subject is now dealt under the new section 10.

We would be happy to advise our clients and clarify the implications arising from the amended CAP Code.

UK Government and Competition and Financial Regulators Research Personalised Pricing Practices

TOPICS: Personalised Pricing, eCommerce, InsuranceTech, Consumer Protection, United Kingdom

The UK Government and the **Competition and Market Authority** ("**CMA**") **has** announced that they are conducting new **research which will explore the practice of retailers targeting online shoppers, and offering each shopper a different price for the same goods and services**. Instead of stating one price for all online shoppers, some retailers offer each of them a personalised price, based on their online "journey".

The research will focus on whether and how personal data, such as address, travel history and marital status, is being used by the retailers, as well as whether such practice is common and how businesses are applying it through different mediums, such as search engines, apps and compassion tools. In addition, it will also examine the extent to which these personalised pricing practices actually prevent shoppers from obtaining the best deals.

The UK's **Financial Conduct Authority** ("**FCA**") has also **announced** that **it has launched a market study to explore how general insurance firms use personalised pricing practices for car and home insurance policies, after the FCA identified hidden discrimination between customers**. The reason for the FCA's market study is to ascertain whether and how it should intervene in order to improve this market. The market study will mainly focus on the outcomes for consumers stemming from pricing practices; the fairness of the outcomes arising from these practices; their impact on competition; and will find remedies to address any harm that might be found by the FCA.

CNIL Imposed GDPR Consent Requirements on an Advertising Network Company

TOPICS: Digital Advertising, Data Protection, The French Supervisory Authority for Data Protection, France

The French Supervisory Authority for Data Protection ("**CNIL**") **has issued a formal warning** to the start-up company Vectaury, according to which the company has failed to meet the conditions for **valid consent under the GDPR**. Vectaury is an advertising network that buys online advertising space for its customers (advertisers) and offers them a tool that enables them to collect geolocation data on devices and browsers of users, and, in turn, processes, for profiling purposes and advertising targeting, geolocation data that it receives via real-time bidding offers, in order to allow the company to purchase advertising space.

CNIL ordered the company delete all data obtained on the basis of invalid consent, and noted that the entire industry should view this case as an example. CNIL has become very active lately in the field of behavioural advertising, as this is the second time within a few months that CNIL has issued a formal warning relating to this type of issue (see our related report here). In both cases, CNIL's enforcement action was focused on the advertiser and not on the publisher.

CNIL stated that Vectaury is unable to demonstrate that the data it collects through real time bid requests is subject to informed, free, specific and unambiguous consent. Although the company provided a short notice explaining that the application collects users' data for the purpose of targeted marketing, and offered users three options - to accept, refuse, or customise their preferences - CNIL stated that Vectaury does not comply with the GDPR requirements, based on the following findings:

- The information provided was insufficient, as it was unclear, used complex terms and not easily accessible;
- Users were not asked to consent to the processing of their geolocation data specifically; and
- The consent obtained was not based on an affirmative answer, as the options were pre-ticked.

During the investigation, the company claimed it used a **template framework for its consent flow that had been created by the Interactive Advertising Bureau ("IAB")**. However, CNIL found that the information provided and the consent obtained using this tool, did not meet the GDPR's requirements for consent. **IAB argued in response that Vectaury did not correctly implement the "Transparency & Consent Framework-complaint" consent management platform ("CMP") framework** and that had it been implemented correctly, some of the most problematic issues raised by CNIL would have been addressed.

CNIL Publishes Rules Regarding Audience and Traffic Measuring in Publicly-Accessible Areas

TOPICS: Audience and Traffic Measuring, Data Protection, The French Data Protection Authority, France

CNIL has published several rules applicable to **devices that compile aggregated and anonymise personal data intended to gauge the audience in a certain space**. CNIL noted that the reason for this publication is the increasing number of companies using devices that collect personal data from mobile devices, in order to advertise in the areas for where the public's presence can be measured, such as in shopping malls.

In shopping malls, for example, such devices collect data from mobile phones and allow the compilation of traffic statistics and analysis of the number of visitors to the mall over a certain period; to model the routes visitors take through the shopping mall and departments; and calculate the rate of repeat visitors.

CNIL divided the discussion into the following three scenarios:

- ***Scenario 1: when data is anonymised within short notice (within minutes of collection):***

  According to CNIL, the short period is defined as the time required for the devices to perform the anonymisation of the personal data, **shall take no more than five minutes** and shall be in accordance with the criteria set out in Opinion 05/2014 on Anonymization Techniques of the former Article 29 Working Party.

  CNIL states that **in this scenario, data controllers can rely on their legitimate interest for processing the personal data under the GDPR. However, CNIL recommends that these controllers provide notice to individuals** according to the layered approach of the Article 29 Working Party guidelines on transparency.

- ***Scenario 2: when the personal data is immediately pseudonymised and then anonymised or deleted (within 24 hours):***

  In this scenario, the **data controllers can rely on a legitimate interest in order to retain the personal data, as long as they provide individuals with prior notice, implement an appropriate mechanism to allow individuals to object to the collection of information, adopt processes to allow individuals to exercise their rights under the GDPR, and implement technical measures to ensure the data protection.**

  CNIL highlights the importance of providing the individuals with the option to oppose the collection and processing of their personal data. Accordingly, companies wishing to install audience-measuring devices shall implement technical solutions in order to enable the objection right in a straightforward manner. CNIL gives several examples of who should exercise this right, which include both a priori and posteriori data collection.

- ***Scenario 3: All other cases:***

  Where the device implemented by the data controller does not meet the abovementioned criteria, **the controller may merely retain the personal data based on individual consent, which can be obtained by any means, and should be informed, freely-given and specific**. The data controller must ensure that the option of withdrawing consent is as easy as it is to provide.

Moreover, CNIL noted that as long as the devices involve the systematic monitoring of individuals, the processing would require a data protection impact assessment prior to implementation, regardless of their scenario classification.

We would be happy to provide further advice and recommendations concerning audience measurement technologies in light of the new regulatory guidelines.

Intel Publishes a Proposed US Federal Privacy Law

TOPICS: Data Protection, Intel, United States

American legislators and stakeholders have reached the understanding that in today's economic and technological environment, certain gaps in legislation, especially in comparison with the EU legislation (in particular the GPDR) must be bridged. In this regard, recent calls from the public, research institutions, private corporations and elected officials are being heard, and [at least in some States] have led to new data protection and privacy legislation being enacted (for more information regarding the privacy legislation of certain States, see our special update here).

As part of this trend, **Intel has released a private draft proposed bill ("the Bill") for a Federal US privacy law**, and launched an online portal where the public can discuss its views and ideas and provide suggestions for the draft legislation. The Bill would override the privacy laws, which have already been enacted in several US states.

Some of the key requirements introduced by Intel's Bill are:

- **Collection limitation**: most uses of data will require a risk/benefit analysis that will restrict a company from using data in a way that may result in a risk for individuals. Individuals also should be able to provide explicit consent for the use of their data;

- **Purpose Specification**: the purpose for which the personal data is processed shall be described clearly and specifically and no later than at the time of the collection;

- **Prohibited uses**: the Bill prohibits the processing of personal data when the company knows, or has reason to know, that the processing of such data will likely violate State or Federal laws or regulation, or deny individuals their rights and privileges under the US Constitution;

- **Security safeguards**: the Bill requires companies to adopt reasonable measures to protect personal data;

- **Openness**: the Bill requires three types of policies in order to ensure the understanding by consumers: (i) an explicit notice when particularly sensitive data is being collected; (ii) a thorough report of the company's use of personal data, in order to enable regulators and advocates to understand the company's practices better; and (iii) a detailed privacy policy; and

- **Engagement with third parties**: the company shall exercise appropriate due diligence of the third party's responsibilities relating to personal data. The Bill also requires a contract in such cases to ensure compliance with the Bill's requirements.

Under the Bill, the Federal Trade Commission ("**FTC**") and the US Attorney would respectively have civil and criminal enforcement authorities. The Bill allows the FTC to impose fines on noncompliant entities up to $1 million in criminal fines or imprisonment of up to 10 years. As far as civil penalties are concerned, companies could be fined by up to $1 billion for not complying.

We will continue to monitor the related developments in the US and update as this important trend continues to develop.

ICO Issues Guidance on Encryption and Passwords under the GDPR

TOPICS: Cybersecurity, Data Protection, Information Commissioner's Office, United Kingdom

The Information Commissioner's Office ("**ICO**") has updated its GDPR guidance ("**the Guidance**") in order to include **security guidance that focuses on encryption and passwords, in the context of taking appropriate technical and organisational security measures** (as required by Article 32 of the GDPR):

Encryption:

The ICO suggests that all organisations should have an encryption policy in place, which will govern the use of encryption and will include guidelines to assist staff training in relation to the use of encryption.

In addition, the organisations must ensure that the planned encryption solution meets current acceptable standards, such as FIPS 140-2 and FIPS 197. Organisations should also be aware of the residual risks of encryption (e.g., by conducting a data protection impact assessment), and take steps to address such risks.

The ICO has stated that when implementing the encryption requirement, organisations shall choose the right algorithm, key size, software and ensure the key is kept secure. **All encryption methods shall be regularly assessed in order to ensure that they remain appropriate.**

The Guidance also addresses the **transmission of personal data**, and suggests that organisations use encrypted communications channels when personal data is transmitted over an untrusted network. The ICO added that in some circumstances, **organisations might be subject to regulatory action if unencrypted data is lost or destroyed.** Here is an example of a recent enforcement measure taken in Germany for a similar reason.

Passwords:

The GDPR states that, in general, personal data must be appropriately protected and does not specifically address the use of passwords as a security measure. According to the ICO's new Guidance, **a good password system is able to protect against two kinds of attacks**: it should be as difficult as possible for attackers to access stored passwords, and it should protect against brute force or guessing techniques.

The Guidance also includes the following issues and recommendations:

- Passwords shall be used only when appropriate. Sometimes a higher level of protection will be required;
- The system should use an appropriate hashing algorithm. Passwords must not be stored in plaintext;
- Login pages must be protected with HTTPS, or an equivalent level of protection;

- Password length should be not less than 10 characters; the system should allow the use of special characters, but should not mandate it, and users should not be allowed to choose common or weak passwords;
- Limitations should be imposed on login attempts; and
- The organisation should consider implementing two-factor or multifactor authentication wherever appropriate.

Although the ICO's Guidance is not binding, compliance is strongly recommended when implementing encryption or password mechanism. **We would be happy to provide further advice and recommendations concerning the new ICO's Guidance.**

The Israeli Privacy Protection Authority Required to Register Email Addresses Databases

TOPICS: Data Protection, The Israeli Privacy Protection Authority, Israel

The Israeli Privacy Protection Authority has published today (28/11) an opinion regarding the question of **whether the data protection requirements set out under the Israeli Privacy Protection Law apply to a digital database that contains individuals' names and email addresses** ("**the Opinion**").

The Privacy Protection Authority has clarified that a database that contains individuals' names and email addresses would be regarded as "personal information" per the Law.

More importantly, while Article 7(2) of the Law excludes "collection that includes only the name, address and method of communication" from the definition of a "database" under the Law (subject to fulfillment of certain conditions), **it was clarified that a database containing individuals' names and email addresses would not fall within this exclusion**, given that email addresses may, in some instances, reveal additional information relating to the individuals (such as private matters or a persons' beliefs).

The practical outcome of this Opinion is that databases containing names and email addresses would be subject to the data protection requirements set out under the Law, including the duty to register a database (subject to the fulfillment of one of the conditions set out under Article 8(c) of the Law).

It should be also clarified that this requirement would apply, inter alia, to databases gathered or recorded by Israeli businesses with respect to their customers and suppliers (both in Israel and abroad).

We would be happy to provide further advice and recommendations concerning the new regulatory Opinion and its practical implications.

The Israeli National Cyber Directorate Publishes Recommendations in Relation to Organisation Readiness for Cyber Crisis and IR Teams

TOPICS: Cybersecurity, Incident Response, The Israeli National Cyber Directorate, Israel

The Israeli National Cyber Directorate has published its **recommendations regarding the establishment, as well the qualifications of crisis management and incident response ("IR") teams in organisations**. The document was published in light of the accelerated growth of cyber-attacks, which might cause significant harm to small organisations, as well as to an entire sector and even at a national level.

The document includes, inter alia, the following key recommendations:

- The IR team shall include a **team leader**, and the team members should know how to handle data collection, data analysis and the blocking of malicious activity. It is also recommended the team include a reverse engineer and malware analysis experts;
- The organisation shall establish **the decision-making process** and communication methods **in advance** in the event of a cyber incident;
- The organisation shall implement **internal policies** which determine mandatory and restricted actions to be taken in case of an incident (such as data retention and deletion, device connectivity, and more);
- The organisation shall map its **core processes** as well as the most important **cyber assets**, and manage their risks accordingly;
- An annual **simulation/exercise** is highly recommended; and
- The IR team shall have **sufficient technology** in order to enable it to respond to a cyber event, such as snipping tools, tools for detection of malicious activities (including anomaly-detection tools), and tools enabling data backup and recovery.

We would be happy to provide further advice and recommendations concerning the Israeli National Cyber Directorate's recommendations and their legal and practical implications.

The Israeli Banking Regulator Publishes New Regulations on Cloud Computing and Technology Innovation

TOPICS: Cloud Technologies, FinTech, Banking, The Israeli Banking Supervision Department, Israel

Easier Conditions for Using Cloud Computing Technologies

The Israeli Banking Supervision Department has announced that it will **allow banks to use cloud computing technologies without having to obtain a special regulatory permission, as they were required to until this announcement**. The reason for taking this step, according to the Banking Supervision Department, is due to the advantages of such technologies and their ability in order to improve their flexibility and response time in the development of new products, improve their services to customers, increase the banks' efficiency, and cooperate with Fintech companies.

The draft amendments to the IT Management Directive **and the** Cloud Computing Directive **have removed the requirement to request permission from the Banking Supervision Department on each occasion prior to implementing cloud technology for several types of applications, such as storage**. Instead, the banking corporation's board of directors and the senior management will bear responsibility for risk management in these cases.

The amended directives state, inter alia, that **each bank's policy must define the material cloud computing, as well as applications for which the management's approval is required, and that a banking cooperation will be required to send to the Banking Supervision Department an annual update of the cloud applications and future applications to be implemented**.

Mandatory Board of Directors Committee for Technology & Innovative

In addition, the regulator has published a draft revision to the Proper Conduct of Banking Business Directive on Board of Directors, which would require the Board of Directors to establish a **dedicated committee for information technology and technological innovation within the Board, and limit the term of the chairmen of Board of Directors committees**.

According to the Banking Supervision Department's announcement, it attributes great importance to accelerating the adaptation of the existing banking corporations to the new world in areas of business innovation based on technology, infrastructure, and the management and use of information, while adjusting risk management.

Therefore, the regulator is encouraging cooperation between the banking corporations and fintech companies to enable the banking corporations to innovate more easily and efficiently, with the aim of increasing value to the customer through better products and services. To achieve these goals, the Banking Supervision Department is acting on a number of levels, including the removal of regulatory impediments (as demonstrated in the amendment to the cloud computing regulations above) and leading broad infrastructure projects.

The amended Directive defines the functions and composition of the committee, as well as its work methods, as follows:

- The committee will deal with a variety of topics connected with the area of **information technology at banking corporation**: the banking corporation's information technology strategy and management policy, technological innovation, appropriate resource allocation for effecting work plans in the areas of technology, preparedness for disaster-recovery after incidents such as cyber-attacks as part of managing the technological risks faced by the banking corporation, and more;

- The committee will emphasise areas of **technological innovation, readiness for the bank of the future, competition created vis-à-vis new technology-based financial actors**, and the new risks faced by the bank due to new activity it intends to undertake and the technologies it intends to adopt. Special emphasis will be placed on **innovation risks in the adoption of new technologies**;

- In addition, the amended Directive includes a requirement to **limit the term of the chairman of a Board of Directors committee**, in order to ensure periodic rotation and renewal that will keep things challenging.

New Google Chrome Version to Fight against Ads from Abusive Sites

TOPICS: Adtech Industry Compliance, Advertising Policies, Unwanted Ads, Google Chrome

Google Chrome's version 71, which is intended to be released in early December, will target **"abusive experiences" advertisements, according to Google's announcement.** "Abusive experiences" are defined by Google as ad impressions that are designed to intentionally mislead or trick users into taking an action they did not intend.

Google has admitted that although last year, the company launched a set of user protection devices against that phenomenon, which have not proved sufficiently effective. **Currently, harmful and misleading ads trick users into clicking them by pretending to be system warnings, or "close" buttons, or are even being used by scammers and phishing schemes in order to steal personal data.**

Google will also allow the sites' owners to check on Google's **special report whether their site contains any of the abusive experiences that need to be corrected or removed**. If the site owners do not act within thirty days, then Google itself will remove said ads.

Dutch Audit Finds Microsoft Office Personal Data Collection Breaks GDPR

TOPICS: Data Protection, The Netherlands

A data processing impact assessment report commissioned by the Dutch government found that **Microsoft breached the European privacy rules. According to the report, Microsoft collects and stores personal data regarding the behaviour of its users without any public documentation.**

The report found that Microsoft collects data on a large scale regarding the individuals' use of its Office software Word, Excel, PowerPoint and Outlook. **Said collection is carried out without providing any prior information, or offering any choice to opt-out, as well as the ability to see what data has been collected.** Microsoft also records and stores individuals' use of connected services, such as translation services through the Office software. The report found that Microsoft collects up to 25,000 types of Office events, data that is made available to up to 30 engineering teams. **In addition, according to the report, the telemetry data collection system sends the data of Dutch users to servers in the US, making it possible for the information to be seized or queried by US law enforcement**.

Moreover, the report states that the qualification of Microsoft as data processor is incorrect. Since Microsoft determines the purposes of the processing and the means of the retention period of such data, Microsoft acts as a controller. **This fact leads to the conclusion that government organisations that enable Microsoft to process personal data, are joint controllers with Microsoft.**

In response to the report, Microsoft announced it is committed to submitting these changes for verification in April 2019 and that in the meantime, the company offers government administrators 'zero exhaust' settings, by which they can shut down the data collection.