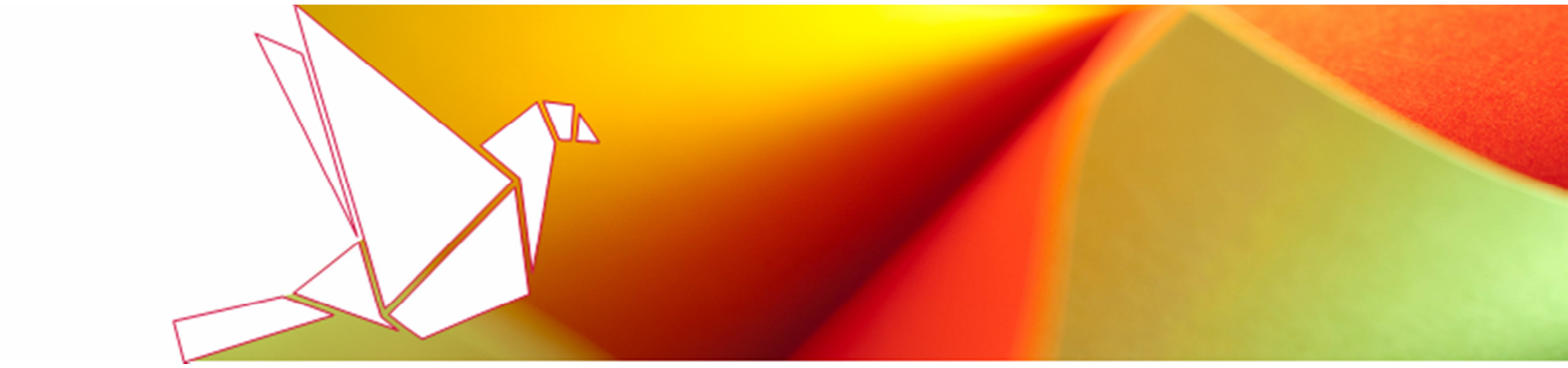


HFN Technology & Regulation Client Update

July 2017

Dear Clients and Friends,

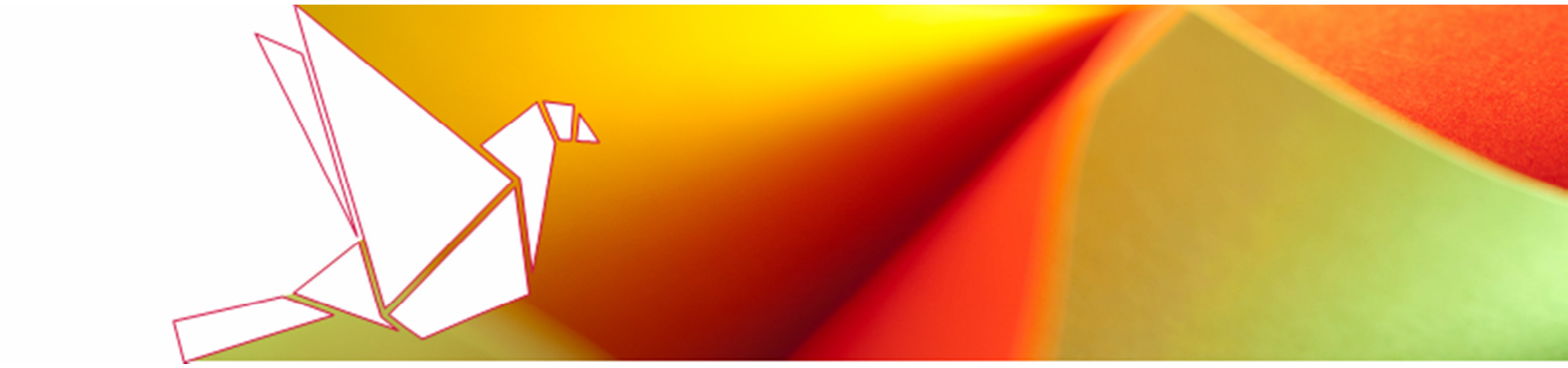
We are pleased to introduce you to our July edition of the Technology & Regulation Client Update, which includes a variety of industry and regulatory developments in the fields of technology compliance, digital advertising, content and information privacy regulations. Amongst other things, you can read about:

- Google's new policies limiting extensions from **changing Chrome settings** and **placing ads on pop-websites utilizing pop-up and pop-under advertisements**;
- FTC's enforcement action against **a lead generation company which unlawfully shared and sold consumers' loan-application sensitive data**;
- The recent updates to **Facebook's Audience Network policies**;
- Instagram's **new tagging tool for influencers and brands regarding sponsored content**;
- Google's initiatives to protect Android users from harmful apps;
- The EU's Article 29 Working Party's new opinion on **data processing at work**;
- ICO's ruling against **hospital which used technology to track patients' symptoms and send alerts to doctors via an application**;
- The ICO's new guidance regarding **subject access requests**;
- The IAB's new **in-app ads standard that includes viewability support**;
- The German parliament's plans **to impose fines of up to €50 million on social media companies over illegal content**.

Kind regards,

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

If you have an important regulatory or industry compliance update you would like to share with the industry, let us know.



Google Tightens Limitations on Changing Chrome Settings

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

Google continues with its efforts to limit extensions from changing various settings on Chrome. About three years ago the company released an extension-based Settings Overrides API for Chrome on Windows which ensures all users have notice and control over any settings alteration that take place in their browser. Thereafter, in March this year, the company implemented similar API for macOS (see our related Client Update).

Following the above, starting from 1 August 2017, the only compliant method to programmatically modify the startup page, homepage, search provider setting, or any other setting which has an API is through the appropriate API. Namely, **if an extension affects changes to any of the above functions, it now must use the formal API.**

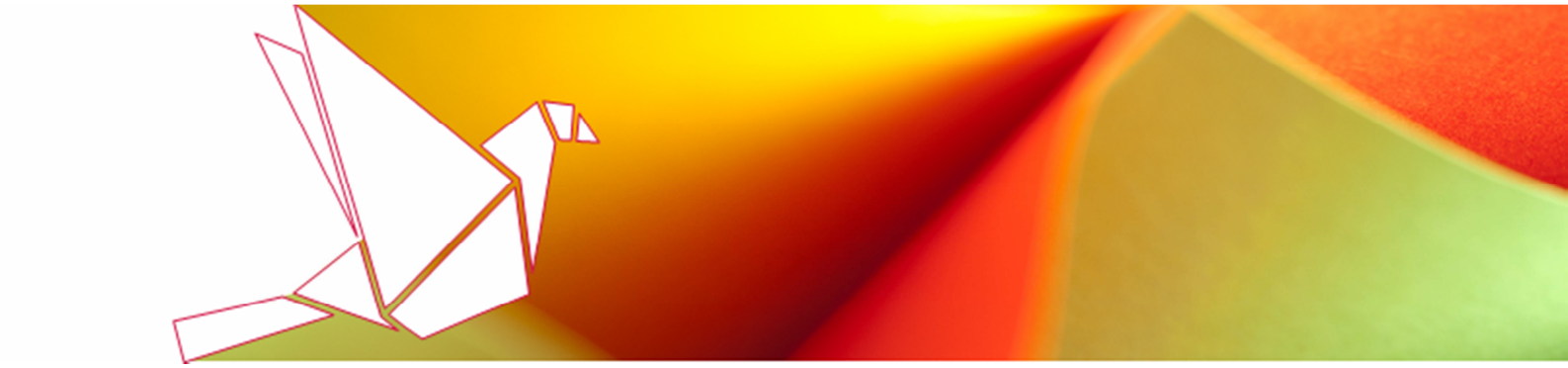
Additionally, extensions which have been using the webRequest API (or other mechanisms) to redirect search requests from the new tab page or the omnibox API, **must now use the search provider or new tab page API.** In other words, **after 1 August 2017, extensions redirecting search requests from the new tab page or omnibox without using these APIs will be removed from the Chrome Web Store.**

Moreover, extensions which perform automatic redirections from a web page URL **must show a prominent notice informing the user of the redirection**. For instance, if an extension redirects search queries from Google (or any other search provider), **the extension's notice must**:

- **Be prominent**: large, conspicuous, and close in proximity to the search box and on the search engine results page;
- **Be timely**: shown prior to the user executing the search;
- **Be persistent**: the prominent notice (including the name) cannot automatically disappear or be dismissable; it must show up every time, not just prior to the first redirect;
- **Must show the name of the extension** (and the brand of search engine, if different) **and what will happen**; and
- **Not look similar to a system or Chrome dialog box or user-interface element**; for instance, disclosures in yellow bars that look similar to Chrome's yellow ("butter") bars are not permitted.

Finally, extensions must also comply with additional Chrome Web Store policies and Google's Unwanted Software Policy.

We would be happy to provide further advice and recommendations concerning the required steps, to ensure compliance with the applicable obligations and their scope.



The FTC Halted Operation Which Unlawfully Shared and Sold Consumers' Loan-Application Sensitive Data

TOPICS: Credit and Loans, Electronic Commerce, Cyber Fraud, Privacy, Security, Consumer Protection, Federal Trade Commission, United States

The operators of a **lead generation business**, Blue Global Media, LLC, have recently agreed to settle charges brought by the US Federal Trade Commission ("**FTC**") that the company deceived consumers into filling out loan applications and sold those applications, which included consumers' sensitive data, to practically anyone willing to pay for the leads.

According to the FTC's complaint, the company and its CEO **operated numerous websites which seduced consumers to complete loan applications**. The company then **sold these applications as "leads" to a variety of entities without regard for how the information would be used or whether it would remain safe and secure**. In addition, the company argued that it would link applicants to the appropriate lenders providing the most favorable loan terms, but instead **indiscriminately sold their information to others, often the first company that offered to pay for it**.

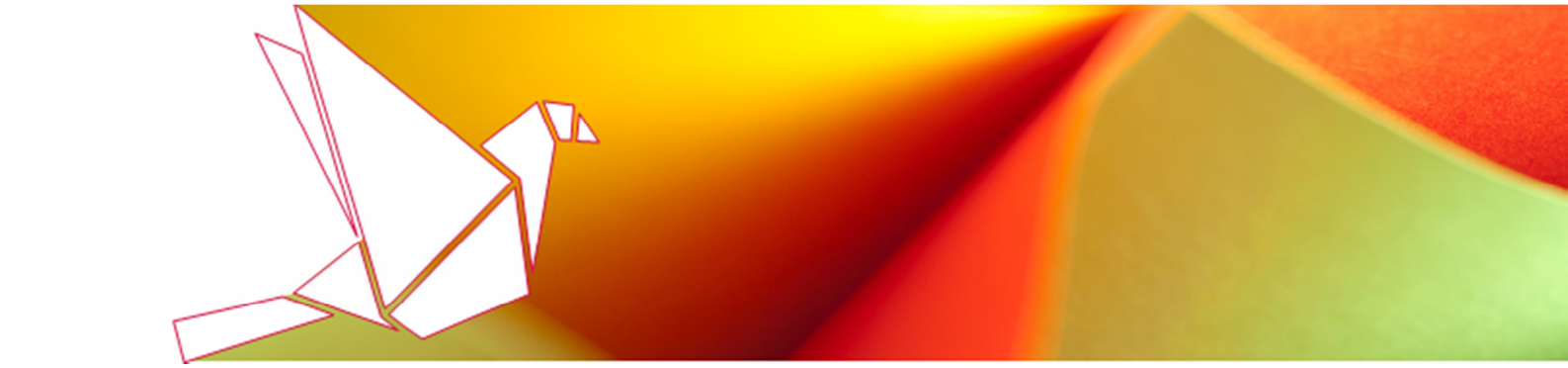
Likewise, the lead generation company promised to defend and secure the sensitive information consumers provided, asserting that the information was only provided to "trusted lending partners". Notwithstanding, the company **provided the complete loan application data submitted by consumers, which included inter alia Social Security numbers and bank account numbers, to any potential buyer without conditions and with little regard to how it would be used**. Furthermore, **the sensitive personal and financial information was shared and sold indiscriminately without consumers' knowledge or consent**. Finally, when consumers complained that their information was being misused, **the company did not investigate or take preventative action**.

As part of the settlement with the FTC, the company is forbidden from misrepresenting that it can assist in providing loans on favorable rates and terms, that it will defend and secure personal information gathered from consumers, and the types of businesses with which it shares consumers' personal information. Under the stipulated order, the company is also **required to investigate and verify the identity of businesses to which they reveal consumers' sensitive information**, and **must obtain consumers' express, informed consent for such disclosures**. Finally, the settlement **includes a judgment for more than $104 million**, which was suspended based on the company's inability to pay.

Facebook Updated Its Audience Network Policies

TOPICS: Adtech Industry Compliance, Facebook, Native Advertising

Facebook has recently updated its Audience Network policies to provide its publishers and developers with a deeper understanding for each policy, the principles which guide them, and how best to implement Audience Network to maximize the performance.



The majority of the recent updates provide more clarity and examples rather than introducing policy changes. However, Facebook has made a **few modifications to its native ad requirements that it is requiring all publishers to comply with by 1 September 2017**. The updated requirements are as follows:

- **Ad title**;
- **Call-to-action (CTA) button** (e.g., Install Now, Learn More);
- **The advertiser creative asset** (for instance: image, video, carousel) or **advertiser icon**;
- **AdChoices icon**;
- **The ad must be clearly labeled and distinguishable from content**; and
- **No longer allowing "whitespace" of native ads to be clickable**.

Failing to comply with the Audience Network policies or to include any of the above advertiser assets in the native ad design could result in Facebook disabling your placement.

Instagram Introduced New Tool to Help Easily Identify Influence Marketing Content

TOPICS: Adtech Industry Compliance, Instagram, Influencer Marketing, Digital Advertising, Online Advertising and Marketing, Federal Trade Commission, United States

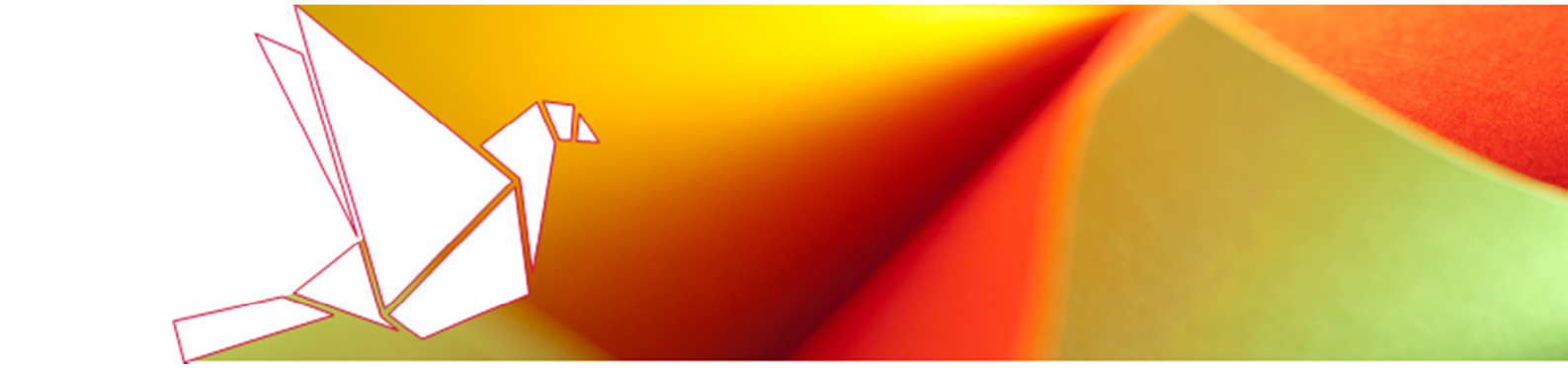
Instagram has recently launched a new feature that would allow celebrities and influencers to make it more conspicuous and clear while they are publishing a post which is sponsored by a brand (in this regard, you can also see our special Client Update titled "Influencer Marketing: Rules of Engagement"). **The new tool will say "Paid partnership with…" at the top of a sponsored posts and Stories**. The new tool will, in the initial stage, be rolled out to only a handful of celebrities and brands.
When the creators and businesses use the "Paid partnership with" tag, they will both have access to Insights to track precisely how their branded content posts and Stories are performing. Creators will continue to see metrics in their Instagram Insights, and business partners will see shared reach and engagement metrics in their Facebook Page Insights.

The FTC has strict guidelines regarding how influencers should disclose the details in advertisements. **It should be as clear and transparent as possible if an influencer is getting paid to post, got free products or services for a post, or has some other business relationship with a brand** (see our related Client Update). It is worth noting that the FTC has recently sent letters to more than 90 influencers and marketers reminding them that they have to clearly and conspicuously disclose when their posts are sponsored (see our related Client Update).

Google Bans Ads on Websites Utilizing Pop-Up and Pop-Under Advertisements

TOPICS: Adtech Industry Compliance, Google, AdSense, Pop-Ups, Pop-Unders

Google has recently announced a change to its advertising policies, **banning pop-up and pop-under advertisements on its AdSense program** (pop-under ads are those which load "under" the current



window, and the user do not see them until they close or minimize their browser window).

Google clarified that **it was no longer permitting the placement of Google ads on pages which are loaded as a pop-up or pop-under**. Moreover, the company said **that it did not permit Google ads on any website which contains or triggers pop-unders, regardless of whether Google ads are shown in the pop-unders**.

Google already has other ad policies around pop-ups, noting that they **are not allowed to interfere with site navigation, change user preferences, initiate downloads, or distribute viruses**. Additionally, **publishers are not permitted to place Google ads on websites which have more than three pop-ups**.

It should be noted that Google has pushed websites down in the search engine results pages for "misbehaving" when it comes to advertisements, as well as has taken other measures in order to eliminate problematic ads (see our related January 2017 Client Update, as well as August 2016 Client Update). Thus, it is very important for publishers to take into consideration the user experience as well as Google's Advertising Policies when considering the advertisements they are using on their websites.

It is recommended for publishers who are using Google ads on their websites to take action to make sure they are complying with Google's updated policies.

Google Rolled Out Play Protect to Defend Against Harmful Android Applications

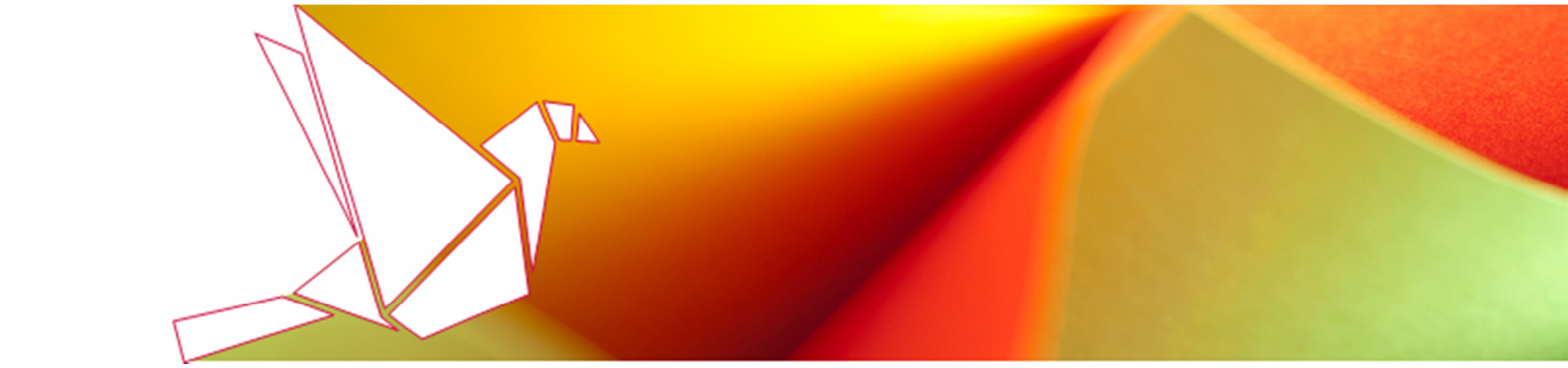
TOPICS: App Industry Compliance, Google Play, Android, Security

Following its announcement back at Google I/O 2017 in May, Google has recently begun rolling out to all Android devices with Google Play Services 11 or higher Play Protect – **comprehensive security services for Android, providing powerful new protections and greater visibility into the device security**.

Google's Play Protect service **automatically scans Android devices** in order to keep the device, data, and apps safe. It should be emphasized that Play Protect **also scans apps which are not downloaded from the Play Store**. Additionally, it provides the users with **detailed information about the security scans**, including the apps which have recently been scanned and the last time that a scan was run. The users can choose to turn off app scanning if they want to for whatever reason.

Applications on the Play Store will also shortly be getting a **"Verified by Google Play Protect" badge**. There will also soon be a **Play Protect card** available in the Updates section of the Play Store from where the users can initiate a manual scan of all the installed apps on their device.

Play Protect is not a new feature per se from Google. The company has long been scanning Android apps on the Play Store and the ones installed on your Android device silently for security risks. Formerly, this feature was frequently known as "Verify Apps" and with this new rebrand, Google is



making its users aware of a security feature which it has been offering to them for years.

The EU's Article 29 Working Party Published Opinion on Data Processing at Work

TOPICS: Data Processing, Employee Monitoring, Privacy, Data Protection Directive, General Data Protection Regulation, Article 29 Working Party, European Union

The EU's Article 29 Working Party ("**WP29**") has recently released its Opinion 2/2017 on **data processing at work**. The opinion, adopted on 8 June 2017, **highlights the challenges and risks of processing employees' personal data in light of new technologies**, and it seeks to provide guidance on balancing employee privacy expectations in the workplace with employers' legitimate interests in processing employee data. **The opinion is applicable to all types of employees and not just those under an employment contract (e.g., freelancers)**.

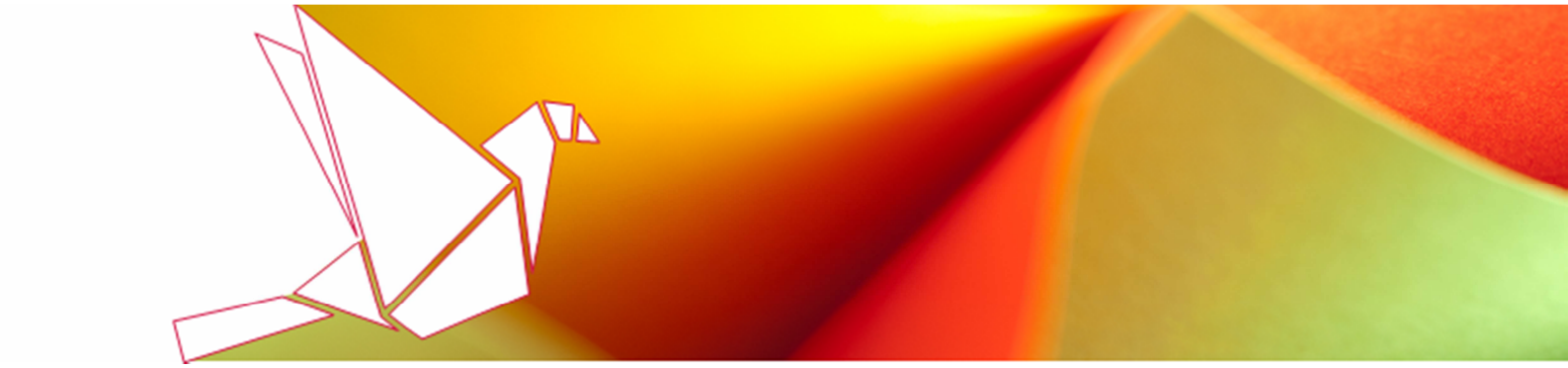
The opinion mainly focuses on the current data protection framework under the EU Data Protection Directive, but also considers the developments as well as some of the obligations arising under the EU General Data Protection Regulation ("**GDPR**") (for further details and recommendations published by us on the GDPR, see our update on How to prepare to the new EU General Data Protection Regulation, as well as our recent GDPR Compliance Playbook).

The WP29's opinion discusses several data processing at work scenarios where new technologies have, or might have, the potential to result in high risks to employees' privacy. Due to the special risks that can arise from the increasing reliance on technologies by employers, the WP29 recommends that in all cases employers should consider, inter alia, whether:

- **Necessity**: the processing activity is necessary, and if so, what legal grounds apply to justify the processing as a matter of data protection law;
- **Fairness**: the proposed processing of personal data is fair to the employees;
- **Proportionality**: the processing activity is proportionate to the concerns raised or the issues meant to be addressed; and
- **Transparency**: the processing activity is transparent to staff.

The WP29's opinion complements its previous Opinion 08/2001 on the processing of personal data in the employment context and the 2002 Working document on the surveillance of electronic communications in the workplace.

We would be happy to provide further advice and recommendations concerning the required steps, to ensure compliance with the applicable obligations and their scope.



The ICO Published an Updated Guidance on Subject Access Requests

TOPICS: Subject Access Requests, Privacy, Data Protection Act, General Data Protection Regulation, Information Commissioner's Office, United Kingdom

The UK Information Commissioner's Office ("**ICO**") has recently issued an updated code of practice on **subject access requests** to reflect developments following two major Court of Appeal judgments published in early 2017 (*Dawson-Damer v. Taylor Wessing LLP* and *Ittihadieh v. 5-11 Cheyne Gardens RTM Company Ltd*). The most significant changes focus on the **disproportionate effort exemption** and subject access requests made for **collateral purposes**.

Under the Data Protection Act 1998 individuals have a right to obtain a copy of the personal data companies hold on them upon filing a request for that information. This also includes employees requesting data held by employers. Those requests are called data subject access requests and must in most cases be complied with within 40 days.

While formerly stating that the disproportionate effort exception should only be relied on in the most exceptional cases, the ICO has slightly soften its stance, with reference to the clarification provided by the Court of Appeal, in determining that, when estimating whether complying with a subject access request would involve disproportionate effort, **a company may take into account difficulties which occur throughout the process of complying with the request, including any difficulties the company encounter in finding the requested information**.

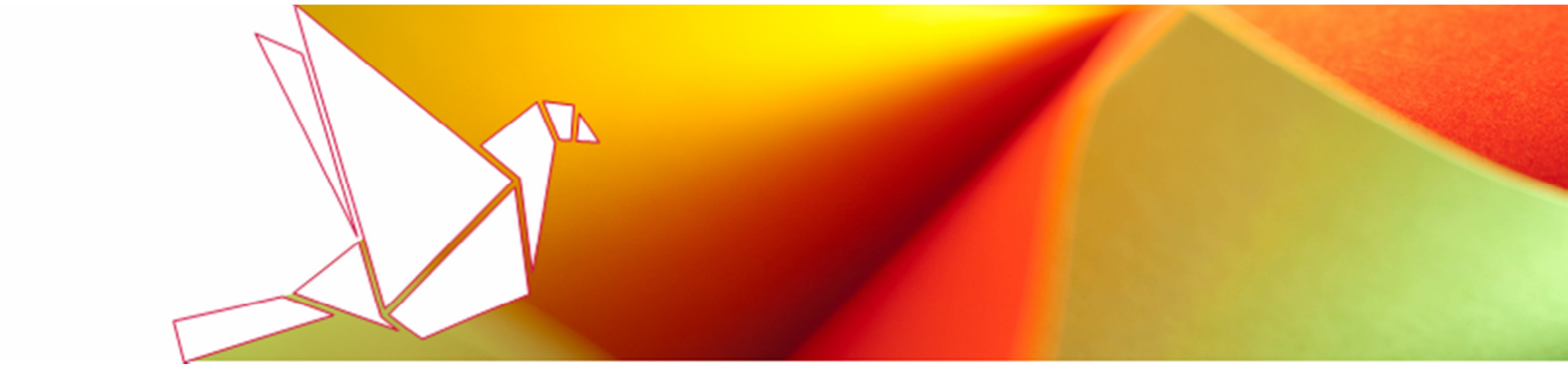
Nevertheless, the ICO expects, inter alia, the **data controller to**:

- **Evaluate the particular circumstances of each request, balancing any difficulties involved in complying with the request against the benefits the information might bring to the data subject**; and
- **Engage with the requester as well as have an open conversation about the information they require**. This willingness to engage with the data subject may be considered by the ICO where a complaint is received regarding the handling of a subject access request.

Moreover, **the burden of proof is on the data controller to show that it has taken all reasonable steps** to comply with the subject access request and that further steps would have been disproportionate.

Additionally, in some instances, subject access requests are made by employees in the context of grievances or to obtain information early in litigation. The ICO's new guidance clarifies that **whether or not a requester has "collateral purposes" for making the subject access request is not relevant in and of itself**, though it will be relevant to the reasonableness of any response (if, for instance, disclosure is due in litigation soon after a subject access request is made, it might well be reasonable to wait and provide the information through the court process).

It should be noted that the GDPR, which will take into effect from 25 May 2018, **will require**



companies to respond to subject access requests in a shorter timeframe than that which currently applies under the Data Protection Act.

The ICO Ruled that Google DeepMind's Deal with the NHS Broke Data Protection Law

TOPICS: National Health Service, Digital Health, Data Protection Act, Privacy Impact Assessments, Google, Ruling, Information Commissioner's Office, United Kingdom

The ICO has recently ruled that the Royal Free London NHS Foundation Trust ("**the Trust**"), which manages a London hospital, failed to comply with the Data Protection Act 1998 when it provided patient details to Google-owned artificial intelligence company DeepMind.

The Trust provided **personal data of approximately 1.6 million patients** as part of a trial to test an alert, diagnosis and detection system for acute kidney injury. Specifically, **the trial used technology to track patients' symptoms and send alerts to doctors through an application called Streams in the event of a drastic change in their health**. According to the ICO's investigation which began in May 2016, there were **several shortcomings in how the data was handled**, including that **patients were not adequately informed that their data would be used as part of the test**.

The Trust has been asked to sign an undertaking committing it to several modifications to ensure it is acting in accordance with the law (see also the Trust's statement which was released on its website following the ICO's investigation). Particularly, the Trust has pledged to:

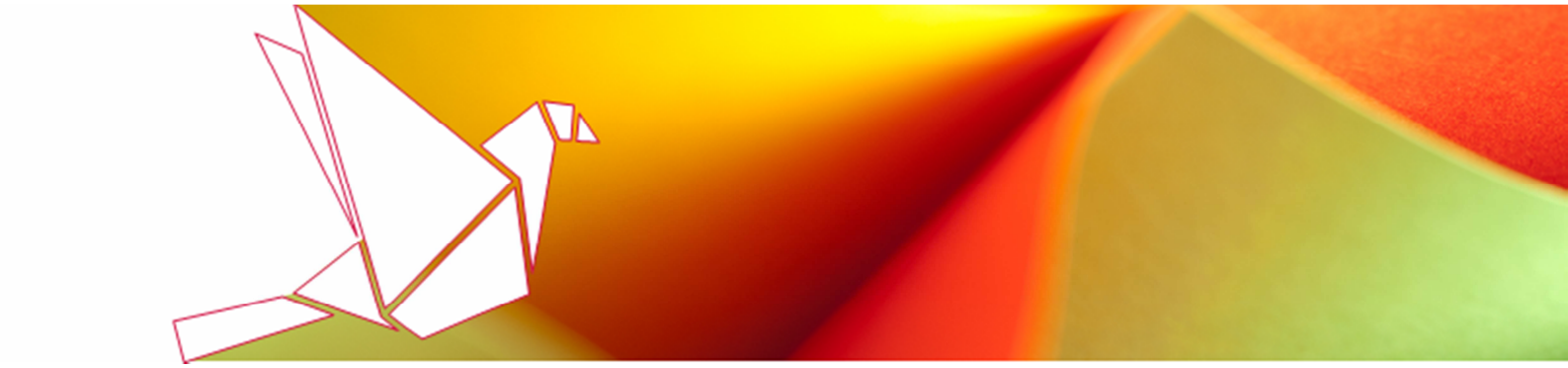
- **Establish a proper legal basis** under the Data Protection Act for the Google DeepMind project and for any future trials;
- **Set out how it will comply with its duty of confidence to patients** in any future trial involving personal data;
- **Complete a privacy impact assessment**, including **specific steps to ensure transparency**; and
- **Commission an audit of the trial**, the results of which will be shared with the ICO, and which the ICO will have the right to publish as it sees appropriate.

The ICO also has published a blog post, reminding the importance of data protection and privacy as well as a few key lessons of its recent investigation.

The IAB Issued a Major Update to Its In-App Ads Standard which Includes Viewability Support

TOPICS: Adtech Industry Compliance, Digital Advertising, Mobile, Standard, The Interactive Advertising Bureau

The Interactive Advertising Bureau's Tech Lab ("**IAB**") has recently released a substantial update to its Mobile Rich Media Ad Interface Definitions ("**MRAID**"), which provides compelling interfaces for the creative to understand where and how it fits in an application, and enables it with a much better way



to deliver the brand's creative experience to the user. This new version (MRAID version 3.0) **remains backwards compatible to all versions of MRAID**.

Highlighted below are some of the **key features** in the new version:

- **Viewability support** that now allows the creative to measure viewability as per industry standards and tailor its display for the best user experience;
- **Audibility measurement** that allows the creative to understand the user's context and use audio in ads in a non-disruptive manner;
- **The standardization of the close button** for expanded ads and interstitials, removes ambiguity, and ensures that the user always has the option to exit an ad;
- Ads can now inform the host ad container if they encounter an error, and initiate a **graceful exit, preserving a clean user experience**;
- Ads can now **access basic information about the environment** like SDK, IFA, COPPA etc., which enables them to prepare the creative in advance of rendering;
- Reduction in the ambiguity in implementation by providing stricter **events implementation sequence** to ensure the ad and the host container are in sync;
- **Guidance for pre-fetched ads**, which ensures that an ad is presented to a user only when it is determined that it has its assets loaded and ready to display;
- **Location data**, when allowed by the user and the app publisher, allows ads to seamlessly use the location data for personalization of creative messaging with MRAID version 3.0; and
- **Video advertising** being among the fastest growing formats, select **Video Player Ad Interface Definition (VPAID) events** are now fully integrated as part of MRAID 3.0 to ensure uniform reporting and measurement of video creative.

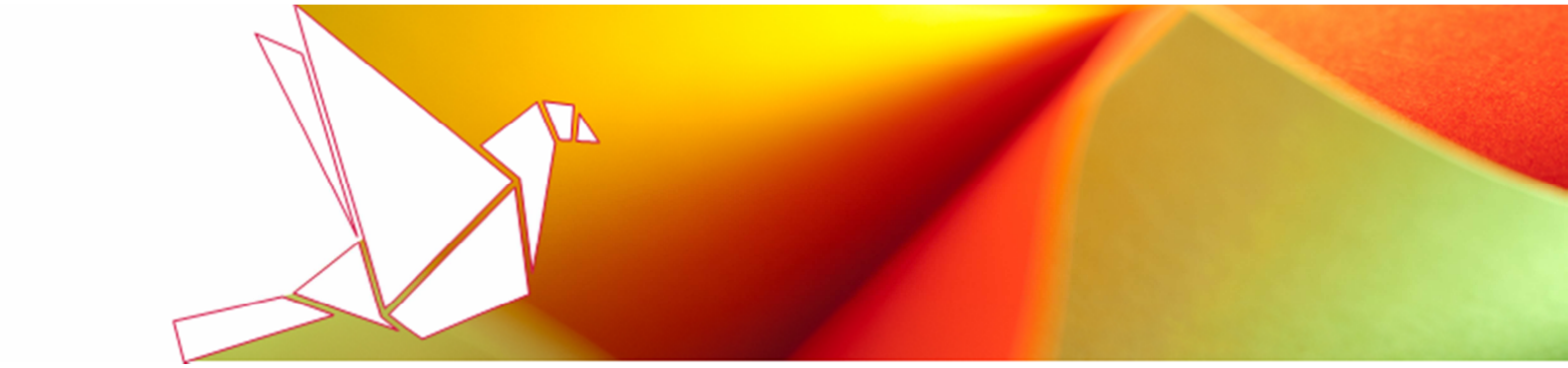
It should be noted that the MRAID standard **is compatible with other industry standards**, such as the Digital Advertising Alliance (DAA) Ad Marker Implementation Guidelines for Mobile.

The MRAID Working Group also intends to release in the coming months a new set of MRAID 3.0 compliance ads to be used for certifying SDKs, as well as to create a best practices guide in order to provide further guidance on how to implement features or clarification of the standard.
We will continue to closely monitor and provide updates on future developments in this field.

German Parliament Approved Plans to Fine Social Media Companies Up To €50 Million over Illegal Content

TOPICS: Social Networking, Digital Media, Fake News, Legislation, Parliament, Germany

According to a recent report on The Guardian, the German parliament has approved **a plan to fine social media companies up to €50 million if they persistently fail to promptly remove illegal content from their websites**, despite concerns the bill could limit free speech online. The law aimed at cracking down on hate speech, criminal material and fake news on social networks.



The law requires social media networks **to remove obviously illegal criminal content within 24 hours** after receiving a notification or complaint, and **to block other offensive content within seven days**. Moreover, it includes **an obligation to report back to the individual who filed the complaint** about how the companies handled the case.

Apart from the hefty fine for companies, the bill also provides for **fines of up to €5 million for the individual each company designates to deal with the complaints procedure if it does not meet requirements**. Social media companies also have **to publish a report every six months** elaborating on how many complaints they received and how they dealt with them.

It should be clarified that a fine would not necessarily be imposed after just one infraction, but only after **a social media network systematically refused to act or does not set up a proper complaint management system**.

Finally, in response to criticism of the draft bill, the government softened the legislation by **excluding email and messenger providers** as well as opening up the option of creating joint monitoring facilities to make decisions concerning what content to remove.

The law will not come into force until after the German federal elections, which will be held in September this year.