Update
Your quarterly Data Privacy and Cybersecurity update

January to March 2019
Welcome to the third edition of Updata – the international quarterly update from Eversheds Sutherland’s dedicated Privacy and Cybersecurity team.

Updata provides you with a compilation of privacy and cybersecurity regulatory and legal updates from our contributors around the globe over the past quarter.

This quarter’s report features commentary on a number of interesting developments, including:

- Updated guidance from the EU’s ENISA on *[What is “state of the art” in IT security?](#)* and a new *[cybersecurity standard on internet-connected consumer devices](#)*.
- New laws in **China**, including a draft specification which updates the *[legal framework regarding personal data collection](#)* and new rules on the *[administration of mobile internet application security verification](#)*.
- The government of **Mauritius** *[emphasising the need to improve law enforcement and the judiciary in the investigation and prosecution of cybercrime](#)* as well as the enhancement of safety and security in cyberspace.
- The government of **Russia**’s approval of new laws which will enable the Federal Service for the Supervision of Communications, Information Technology and Mass Media to conduct *[new types of inspections of personal data operators](#)*, which give more predictability to individuals and businesses.
- **Poland**’s *[first fine issued under the GDPR](#)* for breaches of Article 14’s transparency obligations.

We have also have a number of **Spotlight on...** briefings to share, including commentary on UK Court action: a strategic option for data security breach response, the UAE’s new Healthcare IT Law and the "transfers from EU back into the UK conundrum"
## European Union

### Contributors

**Paula Barrett**  
Co-Lead of Global Cybersecurity and Data Privacy  
*T:* +44 20 7919 4634  
paulabarrett@eversoneds-sutherland.com

**Lizzie Charlton**  
Data Privacy Professional Support Lawyer  
*T:* +44 20 7919 0826  
lizziecharlton@eversoneds-sutherland.com

### Development Summary

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG Opinion on scope of search engine de-listing</td>
<td>Following a previous Court of Justice of the European Union (CJEU) ruling that, subject to exceptions, search engines are required to &quot;de-reference&quot; a webpage, or URL, from their search results when requested to do so by an individual if the webpage in question contains personal data which is inaccurate, inadequate, irrelevant or excessive, Advocate General Szpunar has issued an Opinion in respect of Case C-507/17 Google v CNIL that the CJEU should limit the scope of the de-referencing that search engine operators are required to carry out, to the EU only.</td>
<td>10 January 2019</td>
<td><a href="#">Opinion</a> <a href="#">Press statement</a></td>
</tr>
<tr>
<td>European Union Agency for Network and Information Security (ENISA) report on eIDAS auditing framework for trust providers issuing qualified website authentication certificates</td>
<td>ENISA has published a report assessing the routes to global acceptance of the eIDAS auditing framework for trust providers issuing qualified website authentication certificates.</td>
<td>15 January 2019</td>
<td><a href="#">Report</a></td>
</tr>
<tr>
<td>New PCI Security Standards</td>
<td>The PCI Security Standards Counsel published two new standards, the PCI Secure Software Standard and the PCI Secure Lifecycle Standard (Secure SLC Standard), as part of a new PCI Software Security Framework. The framework is a collection of software security standards and associated programs for the secure design, development and maintenance of modern payment software. The Standards will replace the current PCI Payment Application Data Security Standard (PA-DSS) which will be retired in 2022.</td>
<td>16 January 2019</td>
<td><a href="#">PCI Security Standards blog post</a> <a href="#">PCI Security Standards library</a></td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>ENISA report on security and privacy and the Internet of Things</td>
<td>ENISA has published analysis mapping existing security standards against requirements on security and privacy in the area of the Internet of Things.</td>
<td>17 January 2019</td>
<td>Report</td>
</tr>
<tr>
<td>European Data Protection Supervisor (EDPS) report on smart glasses and data protection</td>
<td>The EDPS has issued a report which aims to clarify the state of play of smart glasses (wearable computer devices with mobile internet connection, to be worn as or mounted on eye-glasses), official positions on related data privacy issues and future developments. The report examines the data privacy issues associated with smart glasses, such as facial and voice recognition and the collection of “invisible” personal data like device identifiers in the form of Wi-Fi or Bluetooth radio signals. The EDPS summarises that given the GDPR provides stakeholders with a harmonised set of principles and a system of tools to assess and control the impact of smart glasses on data privacy, “…an urgent need for technology specific legislative initiatives does not appear to be justified. However, the development of smart glasses and similar connected recording devices underlines the need to establish a robust framework for privacy and electronic communications, as proposed with the ePrivacy Regulation”.</td>
<td>18 January 2019</td>
<td>Report, Press statement</td>
</tr>
<tr>
<td>European Data Protection Board (EDPB) report on second annual joint Privacy Shield review</td>
<td>The EDPB adopted a report on the Second Annual Review of the EU-US Privacy Shield. The report contains commentary on concerns already expressed by the EDPB’s predecessor, the Article 29 Working Party, on the lack of concrete assurances that indiscriminate collection and access of personal data for national security purposes are excluded. In addition, the EDPB notes that the Ombudsperson is not vested with sufficient powers to remedy non-compliance, and that checks regarding compliance with the substance of the Privacy Shield’s principles are not sufficiently strong. The EDPB also highlights additional concerns in relation to checks to comply with the onward transfer requirements, the scope of meaning of HR Data and the recertification process, and a list of remaining issues raised after the first joint review which are still pending.</td>
<td>22 January 2019</td>
<td>Press statement, Report</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| EDPB sixth plenary | The EDPB met on 22 and 23 January for their sixth plenary session. Topics discussed included:  
- Privacy Shield – the EDPB’s report on the Second Annual Review of the EU-US Privacy Shield was adopted (see update below).  
- Brexit – EDPB members agreed to cooperate and exchange information regarding their preparations and the tools available to transfer data to the UK post-Brexit.  
- Clinical trials – the EDPB have adopted an opinion on the clinical trials Q&A, which addresses the adequate legal bases in the context of clinical trials and the secondary uses of clinical trial data for scientific purposes.  
- Data protection impact assessment (DPIA) lists – the EDPB adopted opinions on the DPIA lists submitted by Liechtenstein and Norway.  
- Guidelines on certification – the EDPB adopted the final version of the guidelines on certification. The guidelines explore the rationale for certification as an accountability tool, provide explanations for the key concepts of the certification provisions in Articles 42 and 43 GDPR, explain the scope of what can be certified and outline the purpose of certification.  
- Australian supervisory authority request – the EDPB discussed a written request received from the Office of the Australian Information Commissioner regarding the publication of data breach notifications by supervisory authorities. | 22-23 January 2019 | News update |
<p>| New Open Data and Public Sector Information Directive | The European Parliament, Council and Commission reached agreement on the text of the new Directive on Open Data and Public Sector Information, which sets out the conditions under which public sector non-personal data should be made available for re-use with the aim of making it more easily accessible. | 23 January 2019 | Press statement |</p>
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EU-Japan adequacy agreement</strong></td>
<td>The European Commission and Japan formally adopted a mutual adequacy arrangement enabling personal data to flow freely between the European Union and Japan. The European Commission is also in the process of negotiating an adequacy decision with South Korea.</td>
<td>23 January 2019</td>
<td>Press statement <a href="#">Factsheet</a></td>
</tr>
<tr>
<td><strong>Artificial Intelligence (AI) and data protection</strong></td>
<td>The European Council’s Convention 108 consultative committee has published a set of baseline guidelines on Artificial Intelligence and Data Protection, that governments, AI developers, manufacturers, and service providers should follow the guidelines to ensure that AI applications do not undermine the human dignity and the human rights and fundamental freedoms of every individual, in particular with regard to the right to data protection.</td>
<td>25 January 2019</td>
<td><a href="#">Guidelines</a></td>
</tr>
<tr>
<td><strong>Supreme Court finds government system for disclosing criminal convictions is “disproportionate” and breaches Article 8 ECHR</strong></td>
<td>Unlock (a charity for people with convictions) brought a claim against the Government concerning the way they implement the filtering system for criminal records disclosure, and the fact that it does not comply with Article 8 ECHR (right to respect for private and family life). By way of background, there are three types of criminal record check available in the UK via the Disclosure and Barring Service. The searches are tightly regulated to ensure that they are only made where permitted by law and justified. The type of check which can be conducted and the information that the results of the check will contain, will depend on the relevant role. The Government is now compelled to look at making changes to the rules and processes governing criminal records disclosure.</td>
<td>30 January 2019</td>
<td><a href="#">Judgment</a></td>
</tr>
<tr>
<td><strong>EDPB news: February 2019</strong></td>
<td>The EDPB was involved in a number of projects in February, including: - hosting its <a href="#">seventh plenary</a> on 12 February 2019. The plenary included discussions on Brexit, the 2019-2020 EDPB Work Program, the consultation on guidelines on codes of conduct, the Article 64 GDPR Opinion on the draft AA by the European Securities and Markets Authority (ESMA) and the International Organisation of Securities Commissions (IOSCO).</td>
<td>February 2019</td>
<td><a href="#">Seventh plenary agenda</a> 2019-2020 Work Program Consultation on guidelines on codes of conduct and monitoring bodies Opinion on transfers between EEA and non-EEA countries</td>
</tr>
</tbody>
</table>

*Update Edition 3 - January to March 2019 | Updates by territory*
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>- publishing its <strong>2019-2020 Work Program</strong> – Among other things, the program includes issuing guidance on targeting social media users, reliance on Article 6(1)(b) in the context of online services, the concepts of controller and processor and the notion of legitimate interest of the data controller, video surveillance, data protection by design and default and connected vehicles.</td>
<td></td>
<td></td>
<td>EEA financial supervisory authorities</td>
</tr>
<tr>
<td>- launching a <a href="#">consultation on guidelines on codes of conduct and monitoring bodies</a> under GDPR. The consultation ends on 2 April 2019.</td>
<td></td>
<td></td>
<td>GDPR implementation overview report</td>
</tr>
<tr>
<td>- publishing an opinion endorsing the draft arrangement by ESMA and IOSCO for the <strong>transfer of personal data between EEA financial supervisory authorities and non-EEA financial supervisory authorities</strong>.</td>
<td></td>
<td></td>
<td>Consultation on Annex 2 to certification guidelines</td>
</tr>
<tr>
<td>- publishing a <strong>GDPR overview report</strong> – The report contains some interesting statistics on the implementation of the GDPR and the roles and means of the national supervisory authorities.</td>
<td></td>
<td></td>
<td>Norway and Leichtenstein DPIA lists</td>
</tr>
<tr>
<td>- making the <strong>Norway and Leichtenstein DPIA lists</strong> available online.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- publishing an <a href="#">opinion on clinical trials Q&amp;A</a> – The opinion addresses, among other things, aspects related to the adequate legal bases in the context of clinical trials, and the secondary uses of clinical trial data for scientific purposes.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Latest draft ePrivacy Regulation**

The Romanian Presidency of the Council of the European Union published two further revisions to the proposed ePrivacy Regulation this quarter, ahead of discussions in WP TELE meetings on 19-20 February and 26 February.

Look out for our briefings on the proposed ePrivacy Regulation soon.

- [Draft ahead of 19-20 February meeting](#)
- [Draft ahead of 26 February meeting](#)

---

### Notes

- **Consultation on guidelines on codes of conduct and monitoring bodies**
- **Transfer of personal data**
- **GDPR overview report**
- **Consultation on Annex 2 to certification guidelines**
- **Norway and Leichtenstein DPIA lists**
- **Opinion on clinical trials Q&A**

---

*Update Edition 3 - January to March 2019 | Updates by territory*
### Development

<table>
<thead>
<tr>
<th>ENISA news: February 2019</th>
<th>February 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td><strong>Links</strong></td>
</tr>
<tr>
<td>ENISA publicised the following key updates in February:</td>
<td></td>
</tr>
<tr>
<td>– Guidelines written by German IT security association, TeleTrusT in cooperation with ENISA on <strong>What is “state of the art” in IT security?</strong> The phrase &quot;state of the art&quot; is used in the GDPR Article 32 in relation to the security measures controllers and processors are required to implement.</td>
<td></td>
</tr>
<tr>
<td>– ENISA is encouraging organisations to get involved in <strong>European Cyber Security Month 2019</strong>.</td>
<td></td>
</tr>
<tr>
<td>– <strong>Smartphone Secure Development Guidelines</strong> – ENISA has released SMAShiNG, an online tool that maps security measures for smartphone guidelines. The tool supports developers to build secure mobile applications. SMAShiNG touches upon crucial security measures such as: User authentication; Sensitive data protection; Secure software distribution; Device and application integrity; Protection from client side injections; and Correct usage of biometric sensors.</td>
<td></td>
</tr>
<tr>
<td>– <strong>Internet of Things security checklist</strong> – This new ENISA tool will help users save time when identifying threats and prioritising security areas of importance.</td>
<td></td>
</tr>
</tbody>
</table>

---

### Uploading video content online with identifiable people in the background

<table>
<thead>
<tr>
<th>14 February 2019</th>
<th>CJEU ruling</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td><strong>Links</strong></td>
</tr>
<tr>
<td>In the case of Sergejs Buvīds v. Datu valsts inspekcija (C-345/17), the CJEU ruled that someone who records video footage with identifiable people in the background and uploads that footage to an online platform allowing unrestricted access by third parties falls within the scope of the data protection framework, and outside the domestic purposes exemption. The impact of being within the data protection framework means that the person uploading the video needs to, among other things, register with or notify their national supervisory authority and provide appropriate privacy information to the data subjects in the footage, respond to access requests etc. and fulfil other responsibilities of a controller. The court referred the question of whether the GDPR derogation for journalistic purposes could be applied to &quot;citizen journalists&quot; back to the referring court.</td>
<td></td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>European Telecommunications Standards Institute industry standard on internet-connected consumer devices</td>
<td>The European Telecommunications Standards Institute (ETSI) Technical Committee on Cyber-Security has issued the ETSI industry standard technical specification 103 645 on internet-connected consumer devices. The standard is based on the UK Government’s Code of Practice, which was launched in October 2018 and provided guidance for consumers on how they can help set up and manage their smart devices to improve their safety and protect their personal information.</td>
</tr>
<tr>
<td>Regulation strengthening the security of EU citizens’ ID cards and residence documents</td>
<td>On 19 February 2019, representatives of the Romanian Presidency of the Council and the European Parliament reached informal triilogue agreement on a proposal for a Regulation strengthening the security of EU citizens’ ID cards and residence documents issued to EU citizens and their non-EU family members exercising their right of free movement.</td>
</tr>
<tr>
<td>European Data Protection Board overview report on GDPR implementation</td>
<td>The EDPB published an overview report, in collaboration with the European Parliament’s Civil Liberties, Justice and Home Affairs Committee (LIBE), on the implementation of the GDPR and the roles and means of the national supervisory authorities.</td>
</tr>
<tr>
<td>European Data Protection Supervisor annual report</td>
<td>The EDPS released his 2018 Annual Report, which provides an insight into all EDPS activities in 2018.</td>
</tr>
</tbody>
</table>
| European Data Protection Board 8th plenary | On 12-13 March, the EDPB convened for their 8th plenary. The key outcomes from the plenary were:  
  - Opinion on the interplay between the ePrivacy Directive and GDPR – the opinion seeks to address whether the fact that the processing of personal data triggers the material scope of both the GDPR and the ePrivacy Directive, limits the competences, tasks and powers of data protection authorities under the GDPR. The EDPB opines that data protection authorities are competent to enforce the GDPR. The mere fact that a subset of the processing falls within the scope of the ePrivacy directive, does not limit the competence of data protection authorities under the GDPR. | 12-13 March 2019 | Press statement Opinion on ePrivacy Directive and GDPR interplay ePrivacy Regulation statement Spain DPIA list Iceland DPIA list Statement on political campaigns |
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Commission welcomes provisional agreement to better protect whistleblowers</td>
<td>The European Parliament and the Member States have reached a provisional agreement on rules that will guarantee a high level of protection for whistleblowers who report breaches of EU law. The rules cover anti-money laundering and corporate taxation, data protection, protection of the EU's financial interests, food and product safety and environmental protection and nuclear safety.</td>
<td>12 March 2019</td>
<td><a href="#">Press statement</a></td>
</tr>
<tr>
<td>EU Cybersecurity Act</td>
<td>The European Parliament adopted the EU Cybersecurity Act. It establishes the first EU-wide cybersecurity certification scheme to ensure that certified products, processes and services sold in EU countries meet cybersecurity standards. It also reinforces the mandate of the ENISA, upgrading this to a permanent EU Cybersecurity Agency, so as to better support member states in tackling cybersecurity threats and attacks. The Act was subsequently approved by the European Council at first reading without discussion and has been published in the Official Journal.</td>
<td>12 March 2019 (adopted by Parliament)</td>
<td><a href="#">Press statement</a></td>
</tr>
<tr>
<td>Proposed EU measures to enhance cybersecurity</td>
<td>The EU is stepping up its capacity to protect Europe against cyber threats by creating a new structure to pool and network its expertise in cybersecurity research, technology and industrial development. The Council has granted the presidency a mandate to start talks with the European Parliament on:</td>
<td>12 March 2019</td>
<td><a href="#">Press statement</a> <a href="#">Briefing paper (European Parliament)</a></td>
</tr>
<tr>
<td></td>
<td>- establishing a top knowledge base for cybersecurity, the &quot;European Cybersecurity Industrial, Technology and Research Centre&quot;, which will enhance coordination of research and innovation in cybersecurity; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>Security and privacy considerations in autonomous agents</td>
<td>ENISA released a report, which discusses the main security and privacy considerations of artificial intelligence technology used in autonomous agents in the modern society such as unauthorised autonomous systems, hijacking and misuse transparency and accountability, pervasiveness, retention and opacity of processing. The report also provides a set of recommendations for relevant stakeholders and policy makers, including on supporting the adoption of security and Privacy By Design principles, developing a collaborative approach on the identification and exchange of best practices, endorsing existing initiatives on the protection of human rights through the establishment of appropriate ethical conditions related to autonomous agents, and establishing a relevant framework for policy development, emerging technologies and new application areas.</td>
<td>14 March 2019</td>
<td>Report</td>
</tr>
<tr>
<td>ENISA study on privacy standards for information security</td>
<td>ENISA published a study, which provides insights into the state-of-the-art of privacy standards in the information security context by mapping existing standards available and standardisation initiatives alike.</td>
<td>15 March 2019</td>
<td>Press statement</td>
</tr>
<tr>
<td>EU Law Enforcement Emergency Response Protocol</td>
<td>The Council of the EU has adopted a protocol, which will support EU law enforcement authorities in providing an immediate response to major cross-border cyber-attacks.</td>
<td>18 March 2019</td>
<td>Press statement</td>
</tr>
<tr>
<td>AG opinion on cookies and consent in Planet49 case – referred from German court</td>
<td>In the German case, Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. the Advocate General Szpunar gave an opinion, which echoes the long-held interpretation that pre-ticked boxes do not amount to valid consent for cookies. Notable comments include:</td>
<td>21 March 2019</td>
<td>Opinion (English)</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>– “The activity a user pursues on the internet (reading a webpage, participating in a lottery, watching a video, etc.) and the giving of consent cannot form part of the same act.”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>– “for the purposes of the application of Articles 5(3) and 2(f) of Directive 2002/58 in conjunction with Article 2(h) of Directive 95/46 it makes no difference whether the information stored or accessed constitutes personal data.”</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Austria

#### Development Summary

<p>| Amendment Austrian constitution regarding competence for Data Protection matters (Federal Gazette I. No. 14/2019) |</p>
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Austrian Parliament passed a constitutional law which clarified that (almost) all matters of Data Protection are within the competence of the Austrian Federal Government. The effect is that the Austrian States have (almost) no legislative or administrative competence in matters of Data Protection.</td>
<td>1 January 2020</td>
</tr>
</tbody>
</table>

#### Austrian Data Protection Authority (DPA)

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Austrian DPA published their Quarterly Report - there currently are 134 administrative penal proceedings under GDPR/the Austrian Data Protection Act. However, no significant penalties have been imposed yet. The highest (published) penalty to date was EUR 4,800 for a non-compliant CCTV installation.</td>
<td>11 January 2019</td>
</tr>
</tbody>
</table>

#### Austrian Privacy NGO “nyob” files complaints against 8 streaming services

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Austrian Privacy NGO “none of your business” (nyob), under the leadership of Max Schrems, filed a complaint against eight streaming services (including Netflix, Spotify, Youtube and AppleMusic) for violations of Article 15 GDPR, the right of access.</td>
<td>18 January 2019</td>
</tr>
</tbody>
</table>

#### Austrian Postal Services – Scandal involving sale of...

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigative journalists discovered that the Austrian Postal Services collected a large amount of personal data on almost all Austrians from public and non-public sources. The data was combined to calculate predictions about the data.</td>
<td>12 February 2019</td>
</tr>
</tbody>
</table>
### Austria

#### Development | Summary | Impact date | Links
--- | --- | --- | ---
personal data regarding political affiliation | The Austrian DPA ruled that this behaviour constitutes a violation of both GDPR and Austrian National Data Protection Law. The Austrian Postal Services were ordered to stop processing and delete the data. Furthermore, they were ordered to repeat their Data Protection Impact Assessment and to change entries in their Records of Processing Activities. | 13 September 2018 (decision date) | Decision by the Austrian DPA (in German) |

#### Austrian DPA rules that legal entities have a right to Data Protection

Before the introduction of the GDPR, the Austrian Data Protection Act included a right to data protection for both natural persons and legal entities. When the old Data Protection Act was replaced by GDPR, all references to a right to data protection for legal entities were removed.

As, however, the right to Data Protection is guaranteed as a basic right by the Austrian Constitution, there was debate about whether the right to data protection still applies to legal entities or not.

A recently published judgment by the Austrian DPA clarified that legal entities cannot claim the rights under GDPR. However, based on the Austrian Constitution, legal entities still have a basic right to the protection of their data.

As it is still highly disputed what rights this right to Data Protection of legal entities includes, we are awaiting further clarifications by the Austrian DPA and/or the Constitutional Court regarding its application and scope.

#### Data Breach at Austrian Allergy Treatment Facility - Austrian DPA investigation finds severe GDPR violations

A small Austrian Allergy Treatment Facility filed a data breach notification to the Austrian DPA. Following the notification, the DPA launched an investigation and found several violations of GDPR by the facility, among which are:

- no DPO was appointed, despite being obligatory for such facilities;
- no DPIA was conducted, although this would have been necessary for at least six data processing operations;
- patients were requested to give their consent for medical documents to be transferred via unencrypted emails - such consent is invalid, as security obligations according to Article 32 GDPR cannot be excluded by the data subject’s consent (nevertheless, the DPA stated that the transfer of such data via encrypted email is not obligatory); and

16 November 2018 (decision date) | Decision by the Austrian DPA (in German) |

13 March 2019 (publication date)
the data protection notice given pursuant to Articles 13 and 14 GDPR was insufficient, as (amongst other reasons) it did not clearly indicate which categories of data are collected from the data subject and which are collected from other sources.

It is not known whether an administrative penal proceeding was initiated as well.
Google fined by the CNIL

On 21 January 2019, the CNIL announced its first fine under the GDPR, imposing a record financial penalty of EUR 50 million against Google LLC. Google was sanctioned for lack of transparency, inadequate information and lack of valid consent regarding ad personalisation.

CNIL had received two complaints from consumer associations (None of Your Business and La Quadrature du Net) immediately after entry into force of the GDPR accusing Google of not having a valid legal basis for the processing of users’ personal data in particular regarding ad personalisation services offered on Android equipped devices.

In the context of cross-border processing operations, the CNIL began its investigation by reporting the complaints to the other European Data Protection Authorities (DPAs) in accordance with the one-stop-shop mechanism. The DPAs came to the conclusion that Google did not have a main establishment in the EU, even if it has a European headquarter in Ireland, and that the one-stop-shop was not applicable. Indeed, the authorities analysis was that the Irish headquarter did not have decision-making powers on the processing activities at issue. Consequently, the CNIL was competent to take a decision on the complaints filed.

21 January 2019

Press statement
Further to its online investigations, the CNIL found that Google was not providing easily accessible information to users, infringing the GDPR’s transparency obligation. Essential information was scattered, and sometimes unclear or unintelligible, preventing users from fully understanding the extent of the processing of their personal data and from giving an informed consent where consent was required.

The CNIL also found that Google did not have a valid legal basis for processing user data for the purpose of ad personalisation. Google was relying on consent, however the consent they obtained was not valid. Google was also using pre-ticked boxes in the ad personalisation options where a positive action is necessary. The user was also asked to give a single consent for all the processing activities for which Google was relying on consent, therefore the consent was not specific enough.

Google announced on 23 January 2019 that it was appealing the CNIL’s decision before the Conseil d’Etat (the French supreme administrative court).

### Reinforcement of the cooperation between the CNIL and the DGCCRF

On 31 January 2019, the CNIL and the DGCCRF (French General Directorate for Competition Policy, Consumer Affairs and Fraud Control) reinforced their cooperation protocol (initially signed in January 2011) to offer better protection to consumers in the context of the development of IoT and expansion of e-commerce. These authorities had already cooperated on the processing of personal data by social networks, unfair commercial practices related to compliance with the GDPR and the use of personal data in e-commerce.

The main areas of cooperation they have strengthened include:
- raising consumer awareness of the risks involved in communicating their personal data and disseminating good practices implemented by professionals;
- exchanging more information relating to non-compliance with consumer law and data protection law;

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reinforcement of the cooperation between the CNIL and the DGCCRF</td>
<td>On 31 January 2019, the CNIL and the DGCCRF (French General Directorate for Competition Policy, Consumer Affairs and Fraud Control) reinforced their cooperation protocol (initially signed in January 2011) to offer better protection to consumers in the context of the development of IoT and expansion of e-commerce. These authorities had already cooperated on the processing of personal data by social networks, unfair commercial practices related to compliance with the GDPR and the use of personal data in e-commerce. The main areas of cooperation they have strengthened include: - raising consumer awareness of the risks involved in communicating their personal data and disseminating good practices implemented by professionals; - exchanging more information relating to non-compliance with consumer law and data protection law;</td>
<td>31 January 2019</td>
<td>Press statement</td>
</tr>
</tbody>
</table>
### Development

<table>
<thead>
<tr>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>– carrying out joint controls and pool their expertise in particular regarding investigation techniques; and &lt;br&gt;– jointly proposing actions at the European level, and sharing their analysis on developments in the legislative and regulatory framework regarding protection of consumers and of their personal data. An annual review will be conducted to ensure the follow-up of this cooperation.</td>
<td>14 February 2019</td>
<td>Press statement</td>
</tr>
<tr>
<td>The CNIL announced the new members of its college which is partially renewed. In particular, the CNIL’s former president, Isabelle Falque-Pierrotin is replaced by Marie-Laure Denis who previously worked at the French audiovisual supervisory authority (Conseil Supérieur de l’Audiovisuel) and at the French authority regulating postal and electronic communication (ARCEP).</td>
<td>14 February 2019</td>
<td>Press statement</td>
</tr>
<tr>
<td>If the UK leaves the European Union without a withdrawal agreement in place and provided that the European Commission has not issued any adequacy decision acknowledging that the UK ensures an adequate level of protection, any transfers of personal data to the UK will have to comply with the GDPR provisions applicable to transfers to third countries. &lt;br&gt;On 20 February 2019, the CNIL issued a few recommendations to help French organisations to prepare to a no-deal Brexit. &lt;br&gt;The CNIL recommends organisations follow five steps, in line with the EDPB information note published on 12 February 2019: &lt;br&gt;– carry out a data mapping of the processing operations which involve a data transfer to the UK; &lt;br&gt;– choose the most appropriate safeguard in light of your specific situation; &lt;br&gt;– implement the relevant safeguard before the date of Brexit;</td>
<td>20 February 2019</td>
<td>Guidelines</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td><strong>Development</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Update the internal documentation to mention that data transfers will be made to the UK; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Update information notices provided to data subjects to inform them about such transfers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The CNIL also took the opportunity to remind organisations about the data transfer instruments available to safeguard transfers from the EU to the UK (i.e. Standard Contractual Clauses, Binding Corporate Rules and codes of conduct and certification mechanisms), and that the derogations set out in Article 49 of the GDPR will also be available on an exceptions only basis.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>First trends in the accountability of IT service providers</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For the 2018 edition of the &quot;Sweep&quot; on Privacy accountability, the CNIL published the results of its investigation into the accountability of IT service providers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The CNIL observed that the good practices implemented by IT service providers to meet their new obligations were as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. All the organisations surveyed have carried out analysis to determine the need to appoint a Data Protection Officer;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. The vast majority of companies have also examined the question of their status under the GDPR, i.e. data processor or joint data controller;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Major organisations have put in place comprehensive procedures to disseminate a privacy culture;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. The most advanced organisations have introduced privacy-by-design into their project methodologies; and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5. The majority of the organisations surveyed reported that they had implemented actions to raise awareness of data protection among their employees, ranging from documentation to training sessions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The progress margins identified during the survey were as follows:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Press statement</strong></td>
<td></td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>The CNIL launches free online GDPR training open to everyone</td>
<td>The CNIL launched the free and open MOOC &quot;L'Atelier RGPD&quot; to train people on GDPR. This training tool is mainly addressed to Data Protection Officers (DPOs), future DPOs, and other professionals wishing to understand privacy, and it can be easily followed by anyone curious about data protection. The MOOC is composed of four modules each lasting approximately five hours, with videos, animated and interactive content, free consultation of complementary documentary resources, and examples drawn from the daily issues encountered by companies. There are also some questionnaires, allowing participants to assess their learning outcomes and to receive a certificate at the end of the training.</td>
<td>11 March 2019</td>
</tr>
</tbody>
</table>
**Development** | **Summary** | **Impact date** | **Links**
--- | --- | --- | ---
Concretization of requirements for communication via e-mail | Email communications require (as a minimum) transport encryption, as offered by the well-known European providers as standard. The transport encryption should be implemented in accordance with the technical guideline "BSI TR-03108 Secure E-Mail Transport"; deviations are possible in view of the protection requirements of the data. It should be noted that in the case of transport encryption, emails on email servers are shown as plain text and can always be viewed. For sensitive data, single transport encryption may not be sufficient and additional technical and organizational measures, such as end-to-end encryption, may be required. The subject of the email should not contain any personal information. | January 2019 | Information sheet

The DSGVO as insufficient basis for deletion claims from Google search results | The Higher Regional Court Dresden ruled that deletion of Google search results, based on Article 17 GDPR, is only possible in rare cases if legal infringement is obvious. It is necessary to conduct a comprehensive assessment of legal interests between the interests of the person concerned and the interests of the public. The significance of search engines in the context of public opinion formation is a particular consideration against the deletion of Google search results. | 7 January 2019 | Decision

“Information about the collection of personal data” from the State Commissioner for Data Protection and Information | The guide suitable for small and medium-sized companies provides information on the implementation of the information requirements under Articles 13, 14 and 21 GDPR. It is recommended to divide the notice into two parts: part 1 contains general information on the processing of personal

---

**Contributors**

**Alexander Niethammer**
Partner
T: +49 89 54 56 52 45
alexanderniethammer@eversheds-sutherland.com

**Lutz Schreiber**
Partner
T: +49 40 80 80 94 444
lutzschreiber@eversheds-sutherland.com

**Nils Müller**
Principal Associate
T: +49 89 54 56 51 94
nilsmueller@eversheds-sutherland.com

**Constantin Herfurth**
Associate
T: +49 89 54 56 52 95
constantinherfurth@eversheds-sutherland.com
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security of North Rhine-Westphalia (LfDI)</td>
<td>data and the rights resulting from processing; and part 2 informs about the right of objection to the processing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recent GDPR fine for missing data processing agreement</td>
<td>The State Commissioner for Data Protection and Information Security of the State of Hamburg stated after an inquiry of “Kolibri Image” that the responsibility for drawing up a data processing agreement is also the responsibility of a controller, not just a responsibility of the service provider acting as data processor. Companies that fail to provide such a contract could face a fine of EUR 5,000 as proposed by the LfDI.</td>
<td>20 January 2019</td>
<td>No official statement available</td>
</tr>
<tr>
<td>Scope of a press-right information claim concerning a convicted police officer</td>
<td>The Administrative Court of Dresden obliged the competent authority to provide information to the press about whether a formerly convicted police officer is still within police service and to what extent he has been assigned official duties, after journalists requested the court to do so. However, this information claim of the press is limited to the general information about the employment of that person and does not include specific information on the outcome of the (non-public) disciplinary proceedings and the precise use of this person within the police service. In essence, the Court ruled that the public interest in information protected by Article 5(1) German Constitution prevails over the private interests of the person concerned.</td>
<td>23 January 2019</td>
<td>Press statement</td>
</tr>
<tr>
<td>Urgent motion against the test data transmission for the population census in Germany in 2021 unsuccessful</td>
<td>Germany is obliged to submit statistical data for a planned population census to the European Commission for the reference year 2021. The legal basis for this process is the German Census Preparation Act. This Act shall ensure the quality of data that will be send from the many competent authorities throughout Germany to the central registration office. It also includes the possibility to load (non-anonymized) data of all individuals that have been reported to the Federal Statistical Office into the software for test purposes (by January 13th 2019). The applicants claimed that this may be a violation of their right to informational self-determination (so called Informationelle Selbstbestimmung). Specifically, the transmission of non-anonymised data would allow conclusions about the core area of private life. Therefore, the operation of the Act should be temporarily suspended. The Federal Constitutional Court now rejected this urgent motion. Based on an impact assessment the Court decided that the possible adverse effects for the data subjects do not outweigh such a significant restriction of the legislator’s scrutiny.</td>
<td>6 February 2019</td>
<td>Decision</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>Federal Cartel Office prohibits Facebook from combining user data from various sources</td>
<td>Among other things, Facebook asked their users for permission to collect and merge data from different sources (e.g. Internet, smartphones). This use of data has now been prohibited by the German Federal Cartel Office (FCO). The FCO is concerned about the market-dominant position of Facebook in the field of social networks. Facebook would have abused its strong market position for data collections. The Office also argued that the consents obtained were not voluntary as users have no choice but to agree to the use of data in order to be able to access the services.</td>
<td>7 February 2019</td>
<td>[Press statement (German)] (German)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[Press statement (English)] (English)</td>
</tr>
<tr>
<td>Information claim against Instagram for insults and fake accounts</td>
<td>The District Court of Frankfurt am Main has ordered Instagram to publish personal data (e.g. IP address, date, time, e-mail address of the applicant) after a woman was distressed over the use of her photograph by a fake Instagram account. Initially, Instagram had claimed in front of the Court that the information claim was too far-reaching and that instead only the data needed to enforce a civil suit should be reported. The Court did not follow this argumentation and ruled that Instagram is a social network within meaning of Art. 1(3) of the Network Enforcement Act of 2017. This leads to the obligation of Instagram, under German Telecommunication law, to submit the information in question.</td>
<td>18 February 2019</td>
<td>[Decision] (Decision)</td>
</tr>
<tr>
<td>Federal Court of Justice refers questions to the European Court of Justice regarding obligation to provide information from YouTube in case of copyright infringement by its users</td>
<td>When uploading videos to YouTube, users must register and provide their name, e-mail address and date of birth, and sometimes a phone number. In addition, users must agree to the storage of their IP addresses. Copyrighted films were uploaded to YouTube by three different users, and the owner of the exclusive rights to the films has asked YouTube for information about the users. It is unclear how far the copyright claim is. The Federal Court of Justice has submitted this question to the European Court of Justice.</td>
<td>21 February 2019</td>
<td>[Press statement] (Press statement)</td>
</tr>
<tr>
<td>Website operator not held liable for alleged content management system (CMS) hack</td>
<td>A copyrighted image has been uploaded to a website. When the copyright owner asserted his rights out of court through a written warning, the affected company explained that none of their employees had uploaded the image. Rather, an unknown third party hacked the website, added a subpage and deposited numerous contents (over 39,000 files). The plaintiff saw this as a mere protection allegation and requested an injunction. The district court of Hamburg considered the website operator not breaching</td>
<td>22 February 2019</td>
<td>No official statement available</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>The use of a GPS positioning system for own vehicle fleet violates GDPR</td>
<td>A cleaning company equipped its own company vehicles with a GPS system, which stored any driven routes with start and finish points including the time travelled and the status of the ignition for a period of 150 days. It was not possible to simply switch the system on/off. In addition, the license plates of the affected vehicles were recorded and assigned to the respective operational users. The company justified the use of data for theft prevention and field staff planning purposes, for example, in case of illness. In addition, the company sought consent from employees. The Administrative Court found the previously imposed prohibition order by Lower Saxony’s DPA lawful. The system was inappropriate and the consent ineffective in respect of theft prevention and the co-ordination of staff. The staff were only partially informed about the pursued purposes and the reference to the right of objection was missing.</td>
<td>19 March 2019</td>
<td>Decision</td>
</tr>
</tbody>
</table>
| Advocate General of European Court of Justice: Opt-in is necessary for effective consent on websites | In Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbrauchzentrale Bundesverband e.V., a German lottery provider used a preselected clause on their website that allowed it to use a web analytics service and to set cookies. Whether this represents an infringement should finally decide the federal court. Among other things, he asked the European Court of Justice (ECJ) whether this was sufficient consent for the purposes of Article 4(11) GDPR. In his Opinion, the Advocate General confirmed that an “opt in” is necessary for effective consent. | 21 March 2019 | Opinion (German)  
| | | | Opinion (English) |
| DSGVO has no effect on orders prior to its entry into force | The Federal Administrative Court ruled that the GDPR does not apply to orders that were issued before they came into force. Decisions made before 25 May 2018 will not be retrospectively measured against the new EU legislation. | 27 March 2019 | Press statement |
## Development

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank fined for data accuracy failings</td>
<td>In Resolution of the NADP No. 2019/363/2, the Hungarian data protection authority (NADP) issued a resolution in a case regarding a bank sending SMS messages to a wrong number and not taking appropriate measures to restrict data processing. The bank was fined to HUF 500,000 (approx. EUR 1,550). The NADP highlighted the importance of the principle of accuracy laid down in Article 5 of the GDPR.</td>
<td>8 February 2019</td>
<td>NADP statement (Hungarian language only)</td>
</tr>
<tr>
<td>Credit management company fined for transparency failings</td>
<td>In Resolution of the NADP No. 2019/1841, the NADP issued a resolution in a case regarding the data processing practice of a credit management company. A fine of HUF 500,000 (approx. EUR 1,550) was imposed. The company breached the principle of transparency stated in Article 5 when it refused to provide information of the processing to the data subject. The data subject also asked for the erasure of its data stored by the company. The NADP pinpointed that if a financial institution is legally required to make backups, this is a statutory data management under GDPR, therefore, in the case of a request for erasure, need not be deleted immediately. In case the backups are not legally mandated, the controller needs to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims, as Article 21 details it.</td>
<td>20 February 2019</td>
<td>NADP statement (Hungarian language only)</td>
</tr>
<tr>
<td>City council fined for revealing identity of whistleblower</td>
<td>In Resolution of the NADP No. 2019/596/3, a whistleblower informed the City of Kecskemét about its employer, which also was entity of the city council. As a result, the employer terminated the whistleblower’s employment. In this resolution NADP imposed a fine of HUF 1,000,000 (approx. EUR 3,100) to the City for revealing the personal data of an anonymous informant.</td>
<td>28 February 2019</td>
<td>NADP statement (Hungarian language only)</td>
</tr>
</tbody>
</table>
### Hungary

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Loan provider fined for breaching data minimisation principle</strong></td>
<td>The NADP stated that revealing personal data in this case had no legal basis and is a data protection incident with grave consequences to the data subject. Although the City reported the incident and informed the data subject, it failed to describe the consequences of the data breach.</td>
<td>4 March 2019</td>
<td>[NADP statement](Hungarian language only)</td>
</tr>
<tr>
<td></td>
<td>In Resolution of the NADP No. 2019/2526/2, a loan providing company refused to erase the phone number of the data subject on the basis of the legitimate interest of enforcing its legal claims. The NADP noted that - the interest balancing test should be performed separately for each data processing purpose; - the business interests of the controller cannot automatically override the legitimate interests of the data subject; - prior to further processing, the controller shall provide the data subject with information on that other purpose; and - the company breached the data minimisation principle by retaining the phone number, while it had other ways of contacting the data subject, such as sending a letter. A fine of HUF 1,000,000 (approx. EUR 3,100) was imposed as a result of the breaches.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ministry of Interior ordered to inform data subjects about data security breach</strong></td>
<td>In Resolution of the NADP No. NAIH/2019/721, the users of the Vehicle Service Platform operated by the Ministry of Interior (MoI) could access the personal data of previous owners of the vehicles contrary to the rules of GDPR. The MoI was informed of the breach, yet it failed to communicate the breach of a personal data to the data subject, thus breached GDPR Article 34. The NADP ordered the MoI to inform the data subjects of the breach and the erasure of the personal data unlawfully processed.</td>
<td>19 March 2019</td>
<td>[NADP statement](Hungarian language only)</td>
</tr>
<tr>
<td><strong>Political party fined for data security breach</strong></td>
<td>In Resolution of the NADP No. NAIH/2019/2668, the login credentials of website users of the party Democratikus Koalíció were posted online. The data could be used to determine political orientation; thus the data breach was constituted high risk.</td>
<td>21 March 2019</td>
<td>[NADP statement](Hungarian language only)</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>The NADP imposed a fine of HUF 11,000,000 (approx. EUR 34,500) to the party for its failure to communicate the breach of a personal data to the data subject, laid down in GDPR Articles 33 and 34.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Development Summary

### Data Protection Commission (DPC) opens statutory inquiry into Twitter

On 25 January, the DPC announced that it opened a new statutory inquiry into Twitter (additional to an ongoing inquiry that commenced in November 2018) following notification of the latest data breach received by Twitter on 8 January 2019. The DPC commented that this inquiry will examine a discrete issue relating to Twitter’s compliance with Article 33 of the GDPR (notification of a personal data breach to the supervisory authority).

### DPC issues statement on proposed integration of Facebook, WhatsApp and Instagram

On 28 January, the DPC published a statement on their website regarding the proposed integration of the three platforms. The DPC noted that while they understood this proposal was at a very early stage of development, they had requested from Facebook Ireland an urgent briefing of what was proposed with a view to closely scrutinising the plans – particularly where it involves the sharing and merging of personal data between different Facebook companies.

The DPC commented that previous proposals to share data between Facebook companies have given rise to significant data protection concerns and the DPC noted it will be seeking ‘early assurances’ that all such concerns will be considered. The DPC emphasised that the integration can only occur in the EU if it is capable of meeting all of the requirements of the GDPR.

### DPC calls for adult’s and children’s views on children’s

In December 2018, the DPC began the first stream of a public consultation process aimed at collecting views of adult stakeholders on important data

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection Commission (DPC) opens statutory inquiry into Twitter</td>
<td>On 25 January, the DPC announced that it opened a new statutory inquiry into Twitter (additional to an ongoing inquiry that commenced in November 2018) following notification of the latest data breach received by Twitter on 8 January 2019. The DPC commented that this inquiry will examine a discrete issue relating to Twitter’s compliance with Article 33 of the GDPR (notification of a personal data breach to the supervisory authority).</td>
<td>Ongoing</td>
<td>Press statement</td>
</tr>
<tr>
<td>DPC issues statement on proposed integration of Facebook, WhatsApp and Instagram</td>
<td>On 28 January, the DPC published a statement on their website regarding the proposed integration of the three platforms. The DPC noted that while they understood this proposal was at a very early stage of development, they had requested from Facebook Ireland an urgent briefing of what was proposed with a view to closely scrutinising the plans – particularly where it involves the sharing and merging of personal data between different Facebook companies. The DPC commented that previous proposals to share data between Facebook companies have given rise to significant data protection concerns and the DPC noted it will be seeking ‘early assurances’ that all such concerns will be considered. The DPC emphasised that the integration can only occur in the EU if it is capable of meeting all of the requirements of the GDPR.</td>
<td>Ongoing</td>
<td>Press statement</td>
</tr>
<tr>
<td>DPC calls for adult’s and children’s views on children’s</td>
<td>In December 2018, the DPC began the first stream of a public consultation process aimed at collecting views of adult stakeholders on important data</td>
<td>12 April 2019</td>
<td>Press statement</td>
</tr>
</tbody>
</table>
### Ireland

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>personal data and data protection rights</td>
<td>protection issues concerning children by way of an online consultation document. The second stream of the consultation launched on International Data Protection Day (28 January 2019) and aims to engage children and young people in the classroom by way of a lesson plan specifically designed by the DPC. The DPC has invited all schools to participate using the lesson plan which will help teachers to deliver a lesson on personal data and data protection rights and to facilitate a discussion where students can express their views on important issues. The DPC intends to use the feedback from both streams to shape future guidance in this area.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPC publishes guidance on Transfers of Personal Data from Ireland to the UK in the event of a 'No-Deal' Brexit</td>
<td>On 8 February 2019 the DPC published updated guidance aimed to assist Irish organisations that transfer personal data to the UK (including Northern Ireland) in the event of a 'No-Deal' Brexit. The DPC noted that in a no-deal scenario, the UK will no longer be a member of the EU and instead will become a 'Third Country' which means transfers of personal data from Ireland to the UK will be treated in the same way as transfers to countries such as Australia, India or Brazil. In practice, this means that in order to comply with GDPR an Irish company intending to transfer personal data to the UK will need to put specific safeguards in place to protect the data in the context of its transfer and subsequent processing - usually by way of Standard Contractual Clauses. Further information can be found on the DPC website.</td>
<td>Ongoing</td>
<td>Guidance</td>
</tr>
</tbody>
</table>
| DPC publishes first Annual Report since GDPR covering the period 25 May - 31 December 2018 | The report was published on 28 February detailing the work of the Irish DPA following the introduction of the General Data Protection Regulation (GDPR) on 25 May 2018. Some highlights include:  
  - 56% increase in total number of complaints compared to 2017;  
  - 70% increase in total number of valid data security breaches recorded compared to 2017;  
  - 136 cross-border processing complaints were received by the DPC through the new 'One-Stop-Shop' mechanism that were lodged by individuals with other EU data protection authorities;  
  - Almost 31,000 contacts were received through the DPC's Information and Assessment Unit.                                                                 | 28 February 2019  | Report     |
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Privacy Enforcement Network (GPEN) 2018 ‘Sweep’</td>
<td>The GPEN’s annual intelligence gathering operation (‘Sweep’) examined organisations’ self-reporting of their implementation of the core concepts of accountability. Participating GPEN members made contact with 356 organisations in 18 countries during the ‘Sweep’ and the results are highlighted within the report. In general, there were examples of good practice reported, but it was found that a number of organisations reported that they had no processes in place to deal with the complaints and queries raised by data subjects and were not equipped to handle data security incidents appropriately. In Ireland, the Sweep was conducted by contacting 30 randomly-selected organisations across a range of sectors. Further information can be found within the 2018 International Report.</td>
<td>5 March 2019</td>
<td>DPC comments Report</td>
</tr>
</tbody>
</table>
# Development Summary

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public consultation on general authorization</td>
<td>The Italian data protection authority (IDPA) issued an official Press statement communicating the beginning of a public consultation regarding the measure, distinguishing the provisions of the General Authorizations to the processing of personal data in certain contexts, which are compatible with the GDPR and the Legislative Decree 101/2018, bringing the reformation of the Italian Data Protection Law.</td>
<td>11 January 2019</td>
<td>IDPA's Press statement (Italian language only)</td>
</tr>
<tr>
<td>Publication of deontological rules</td>
<td>IDPA announced the publication in the Italian Official Journal of deontological rules, to be annexed to Legislative Decree 196/2003 (Italian Privacy Code) in various contexts: deontological (ethical) rules for journalists; deontological rules for data processing for statistical and scientific research purposes (including in the context of the Italian national statistical system); deontological rules for data processing to carry out defensive investigations or to exercise or defend a right before courts; and deontological rules for processing for archiving purposes in the public interest or for historical research purposes.</td>
<td>16 January 2019</td>
<td>IDPA's Press statement (Italian language only)</td>
</tr>
<tr>
<td>Explanatory leaflet</td>
<td>IDPA published a leaflet summarising the outcomes of the first months of application of the GDPR in Italy (25 May-31 December 2018).</td>
<td>30 January 2019</td>
<td>IDPA's leaflet (Italian language only)</td>
</tr>
<tr>
<td>IDPA's Newsletter N° 449 of 7 February 2019</td>
<td>IDPA published its newsletter mentioning the following:</td>
<td>7 February 2019</td>
<td>IDPA's response</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IDPA's explanatory page</td>
<td>IDPA answered to the questions by the Italian professional association of labour consultants regarding their privacy roles.</td>
<td></td>
<td>(Italian language only)</td>
</tr>
<tr>
<td>IDPA's explanatory page</td>
<td>IDPA published an explanatory page, also referring to EDPB's notes, regarding data transfers in case of a “Hard Brexit”.</td>
<td>18 February 2019</td>
<td>IDPA’s page (Italian language only)</td>
</tr>
<tr>
<td>IDPA's Newsletter N° 451 of 25 March 2019</td>
<td>IDPA published its newsletter mentioning the following:</td>
<td>25 March 2019</td>
<td>IDPA’s measure (Italian language only)</td>
</tr>
<tr>
<td></td>
<td>− IDPA issued a general measure regarding data protection in the healthcare sector, given the innovations – some of which still in progress - as a consequence of the GDPR and of the amendment of Italian Data Protection Law, to favour a standardized interpretation and application. Such measure is complemented by an explanatory leaflet;</td>
<td></td>
<td>IDPA’s leaflet</td>
</tr>
<tr>
<td></td>
<td>− IDPA issued its investigation plan for the first semester of 2019. IDPA declared that its investigations will be focused in particular on data processing carried out by some categories of public and private subjects, including banks, companies carrying out marketing activities and companies carrying out profiling activities of data subjects adhering to fidelity card programs. IDPA’s controls will also regard lawfulness conditions of the processing, provision of appropriate information notices and data retention periods. In such investigation activities, IDPA may also avail of the dedicated Privacy Corp of the Italian Tax Police. The above is without prejudice to further investigations and controls that IDPA may carry out, also as a consequence of reports and complaints, or under art. 62 GDPR;</td>
<td></td>
<td>IDPA’s decision (Italian language only)</td>
</tr>
<tr>
<td></td>
<td>− In the context of the Council of Europe and of the Convention 108/1981 on data protection, the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, issued the Guidelines on Artificial Intelligence and Data Protection, stating some relevant principles. IDPA prepared an Italian version of such guidelines.</td>
<td></td>
<td>Guidelines on AI and data Protection (Italian version)</td>
</tr>
</tbody>
</table>
## Lithuania

**Contributors**

**Rimtis Puisys**  
Partner  
T: +370 5 239 2373  
rimtis.puisys@eversheds.lt

**Linas Mockevicius**  
Associate  
T: +370 5 239 2391  
linas.mockevicius@eversheds.lt

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lithuanian State Data Protection Inspectorate recommendations regarding data transfers in the event of a no-deal Brexit</td>
<td>The Lithuanian State Data Protection Inspectorate recommends that data controllers and processors transferring data to and receiving data from UK, take preparatory steps for a no-deal Brexit scenario. The Inspectorate points out that in case of a no deal Brexit, the UK will be considered as a third country for the purpose of data transfers, and as such, organizations will be under obligation to comply with the GDPR’s requirements governing the transfer of data outside of the EEA countries, including implementation of appropriate safeguards, such as Standard Contractual Clauses.</td>
<td>No-deal Brexit</td>
<td>Press statement</td>
</tr>
</tbody>
</table>

| Lithuanian State Data Protection Inspectorate plan for preventive audits for 2019 | On 4 February 2019, the preventive audits plan of the Lithuanian State Data Protection Inspectorate has been adopted. According to the plan, it is expected to conduct 75 planned audits. Most of the audits will be carried out in the following types of organization:  
- sports clubs: concerning the legality of processing of biometric data;  
- sport and tourism goods and services companies: concerning the implementation of data minimisation principle when processing the personal data for the purpose of conclusion and execution of rent agreements and provision of information to data subjects about the personal data processing;  
- hotels: concerning the implementation of data minimisation principle while processing the guests’ personal data;  
- public authorities: concerning the agreements, concluded with data processors; and  
- consumer credit entities: concerning security of data processed for the purpose of conclusion and execution of consumer credit agreements. | 4 February 2019 | Press statement |
These controllers were chosen for audit due to the new requirements for the processing of biometric data, as established in the GDPR, due to the claims of data subjects’ and having regard of the results of public opinion polls re data processing, as conducted in Lithuania.

The companies referred to in the audits plan are recommended to prepare for the audits. Noteworthy, that other companies may be audited as well, even if not mentioned in the plan for audits.

The Lithuanian State Data Protection Inspectorate approved the list of data processing operations, which are subject to a data protection impact assessment.

Some of the most relevant cases provided in the list include the situations when:

- processing of personal data takes place when video surveillance is conducted along with sound recording, or at healthcare, social care, detention establishments and other agencies where services are provided for vulnerable data subjects, and in certain other cases;
- recording of telephone conversations takes place;
- processing of personal data of children for direct marketing purposes takes place, or in case of assessment of personal aspects of children which is based on automated processing, including profiling; and/or
- processing of personal data of employees takes place for the purpose of monitoring or control over employees: processing of personal video and/or sound data in a workplace and/or data controller’s premises or territories where its employees work; processing of personal data related to monitoring of employees’ communication, behaviour, place or movement.

The approved list is without prejudice to the scope of GDPR and the cases prescribed therein that the DPIA shall be performed.
# Poland

## Development Summary

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard contractual clauses for the data processing</strong></td>
<td>The Polish data protection authority (PUODO) intends to adopt standard contractual clauses for the matters referred to in Articles 28(3)-(4) (pursuant to Article 28(7)) GDPR. The scope of the clauses will include inter alia how to document the data processing instructions from the controller, how to verify confidentiality obligations by persons authorized to process data, how precisely should the security measures be indicated in the data protection agreement, how to comply with the obligation to provide the information necessary to ensuring the compliance with the obligations pursuant to Articles 32-36 GDPR, how to ensure compliance of the processing the personal data by another processor with the provisions of the data processing agreement concluded with the controller.</td>
<td>14 January 2019</td>
<td>Press statement</td>
</tr>
</tbody>
</table>
| **Sector audits of the PUODO** | PUODO published the yearly plan of sectoral audits. The plan includes the following sectors:  
- Private sector – telemarketing, data brokers in the scope of the legal basis of the processing the personal data, profiling in the banking and insurance.  
- Education – CCTV usage.  
- Employment – CCTV usage, data processing in regard to the recruitment.  
- Healthcare – disclosing personal data in regard to patient’s right to obtain a copy of the medical documentation. | 24 January 2019 | Press statement        |
<p>| <strong>First fine in Poland for GDPR non-compliance</strong> | PUODO imposed its first fine under the GDPR for failure to fulfil the information obligation in accordance with the Article 14 GDPR. The controller was a data broker collecting and disclosing business data to its customers. The PUODO’s investigation focussed on the processing of business to business (B2B) data obtaining by the controller from the public sources | 26 March 2019  | Press statement        |</p>
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
</table>

only, particularly from the public registers of entrepreneurs and companies. The relevant personal data comprised information relating to sole entrepreneurs and board members of the companies. The controller addressed its GDPR information obligations via email to individuals whose email addresses were stored in the controller’s database. As for the remaining individuals, the controller published certain information on its website – the controller decided not to send letters by post. During the proceedings, the controller referred to the exemption in Article 14(5)(b) GDPR, citing that sending about 6.6 million letters to sole traders (the number of the data records without email address in the controller’s B2B database) would involve a disproportionate effort and would cost an estimated PLN 33 million (approx. EUR 7.7 million) having regard to the type of data subjects (professionals). The PUODO didn’t support the controller’s interpretation. Pursuant to the PUODO’s decision, the controller should have fulfilled the information obligation in relation to the data subjects, that is it should have informed them about the controller’s processing of their personal data and provided the outstanding information in accordance to the Article 14(1)-(3) GDPR. The controller plans to contest the decision through the courts.

The controller is a local entity of a European data broker which has companies in 16 European countries, and is a business partner of one of the biggest American corporate data brokers.

The fine totalled PLN 943,000 PLN (approx. EUR 220,000) which is around 4% of the controller’s annual turnover.

The PUODO’s decision is controversial in many respects, particularly in light of a previous decision about the processing of personal data of company board members by another data broker. In that previous decision, the PUODO stated that where the controller does not process the private postal addresses of the board members, it is not obliged to fulfil the information obligation. The fact that the controller processed the corporate postal addresses of the board member data subjects, which could have been used to meet the information obligation, was not taken into consideration.
## Contributions

### Romania

#### Contributors

**Mihai Guia**  
Managing Partner  
T: +40 21 31 12 56 1  
mihagiuia@eversheds.ro

**Alexandra Sulea**  
Senior Associate  
T: +40 21 311 2561  
alexandrahusar@eversheds.ro

**Irina Vascan**  
Junior Associate  
T: +40 21 311 2561  
irinavascan@eversheds.ro

### Development

<table>
<thead>
<tr>
<th>Law no. 363/2018 on the processing of personal data by the competent authorities for crime prevention, investigation, detection and prosecution</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>This new law has entered into force in Romania. It transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.</td>
<td>7 January 2019</td>
<td><a href="#">Official register (Romania)</a></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Law 362/2018 on ensuring a common high level of security of the networks and information systems</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
</table>
| This new law transposes Directive (EU) 2016/1148 concerning measures for a common standard of security for network and information systems across the EU and has been published in Romania’s Official Gazette.  
The public authority in charge of the implementation of this law is CERT-RO / The Romanian National Computer Security Incident Response Team.  
The law establishes notification obligations for security incidents, both mandatory for providers of essential services and voluntary, for other operators. Additionally, the providers of essential services are required to register at the Registry of Essential Services maintained by the public authority. | 12 January 2019 | [CERT-RO press statement](#) |
### Development

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
</table>
| Schengen Data Protection Act| The Schengen Data Protection Act (SDPA) is intended as a transitional law (until the full revision of the data protection law is finalized) to bring Swiss law in line with European legislation. It gives the Federal Data Protection and Information Commissioner (FDPIC) investigative powers and the authority to issue rulings within the framework of the application of the Schengen acquis in criminal matters. The SDPA applies in particular to the processing of personal data by federal bodies in criminal matters. The SDPA does not apply to cantonal authorities. The SDPA introduces the following concepts and points to note:  
  - sensitive personal data includes genetic and biometric data that uniquely identify a person;  
  - the term 'profiling' replaces the term 'personality profile';  
  - data protection through technology and data protection-friendly default settings (privacy by design and default);  
  - rules on automated individual decisions;  
  - under certain circumstances, federal bodies must conduct data protection impact assessments and, in certain cases, consult the FDPIC;  
  - federal bodies must report data breaches to the FDPIC that are likely to pose high risks to the fundamental rights of the person concerned;  
  - the FDPIC can open new investigations and issue rulings as an administrative measure.  
  It is expected that the above provisions will be introduced in the revised Federal Act on Data Protection. | 1 March 2019 | Schengen Data Protection Act text in German                                                                                                                                                                                                                                               |
**Community**

**Paula Barrett**  
Co-Lead of Global Cybersecurity and Data Privacy  
*T:* +44 20 7919 4634  
paulabarrett@eversheds-sutherland.com

**Lizzie Charlton**  
Data Privacy Professional Support Lawyer  
*T:* +44 20 7919 0826  
lizziecharlton@eversheds-sutherland.com

---

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UK data protection legal regime post-Brexit</strong></td>
<td>The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419 (<strong>DPPECRs</strong>) and the associated statutory instrument which amends them, use powers conferred by the European Union (Withdrawal) Act 2018 (<strong>Withdrawal Act</strong>) to merge the EU GDPR and the applied GDPR regimes currently set out in the Data Protection Act 2018, creating a single data protection regime in the UK after exit day – the <strong>“UK GDPR”</strong>. The DPPECRs mirror the extra-territorial scope found in the EU GDPR so that non-UK controllers or processors processing personal data of UK residents will be covered by UK GDPR in certain circumstances. The DPPECRs also, among other things, confer powers on the Secretary of State to make adequacy regulations and to issue Standard Contractual clauses and authorise Binding Corporate Rules. You can find out more about the impact of Brexit on data protection issues in our <a href="#">briefing</a>.</td>
<td>Exit day (UK leaves the EU)</td>
<td>Eversheds Sutherland briefing, Withdrawal Act, DPPECRs, DPPECRs (No 2)</td>
</tr>
</tbody>
</table>
| **Privacy Shield and Brexit FAQs** | The US Department of Commerce has published FAQs on Privacy Shield and Brexit explaining steps certification participants must take to receive personal data from the UK post-Brexit. In order to receive personal data from the UK in reliance on the Privacy Shield, participants must complete certain steps before: (i) in the event the Withdrawal Agreement is agreed – the end of the transition period (31 December 2020); or (ii) in the event of no-deal, 29 March 2019. The steps to be completed are:  
  i. Update your public commitment to comply with the Privacy Shield to include the UK. (Note: If you plan to receive Human Resources (HR) data from the UK in reliance on Privacy Shield, you must also update your HR privacy policy) | Exit day (UK leaves the EU) | FAQs statement |
### United Kingdom

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
</table>
| **UK data protection legal regime post-Brexit** | DCMS guidance  
The Department for Digital, Culture, Media & Sport (DCMS) has published guidance to help stakeholders prepare for a no deal Brexit.  
The guidance explains the amendments which will be made to UK data protection law upon the UK’s departure from the EU under the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (DPPECRs). The DPPECRs were originally laid before Parliament in December 2018, were subsequently changed and laid again on 14 January 2019 to correct minor typos. They amend UK data protection legislation with the aim of ensuring that the UK legal framework for data protection continues to function correctly after exit day.  
The DPPECRs use powers conferred by the European Union (Withdrawal) Act 2018 (Withdrawal Act) to merge the EU GDPR and the “applied GDPR” regimes currently set out in the Data Protection Act 2018 (DPA 2018), creating a single data protection regime in the UK after exit day – the “UK GDPR”.  
Keeling schedules  
DCMS has helpfully published two “keeling schedules” which show (in Tracked Changes) how the DPPECRs will amend the GDPR and the DPA 2018 post-Brexit.  
DPPECRs amendments  
The draft Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) (No 2) Regulations 2019 (DPPECRs No 2) amend the draft DPPECRs to ensure that UK to US data transfers reliant on the Privacy Shield framework are not impinged should the UK leave the EU without a Withdrawal Agreement (no deal scenario). They provide that such data transfers may only take place if the certified Privacy Shield organisation has updated its privacy policy to refer to personal data transfers from the UK, as already confirmed by the US Department of Commerce in their Privacy Shield and Brexit FAQs (as previously reported in January’s bulletin).  
European Data Protection Board (EDPB) | Exit day (UK leaves the EU) | DCMS guidance and keeling schedules  
Withdrawal Act  
DPPECRs  
DPPECRs (No 2)  
DPPECRs amendments and Explanatory memorandum  
Privacy Shield Brexit FAQs  
EDPB guidance on BCRs  
EDPB guidance on data transfers |
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
</table>
| Government report on disinformation and fake news| The EDPB has published new guidance on: (1) Binding Corporate Rules (BCRs) if the UK leaves the EU without a deal in place and the ICO no longer has a role in the BCR community; and (2) data transfers under the GDPR.  

Government report on disinformation and fake news | As reported in Competition section above, the DCMS Commons Select Committee published its final report on Disinformation and fake news. The report finds that electoral law ‘not fit for purpose’ and calls for:  

- a compulsory Code of Ethics for tech companies overseen by independent regulator;  
- a regulator given powers to launch legal action against companies breaching code;  
- the Government to reform current electoral communications laws and rules on overseas involvement in UK elections; and  
- social media companies to be obliged to take down known sources of harmful content, including proven sources of disinformation.                                                                                                                                                                                                                                                                                                                                                           | 18 February 2019  | DCMS report |
| Code of conduct for data-driven health and care technology | The Government and NHS England have developed a Code of conduct for data-driven health and care technology which sets out the behaviours expected from those developing, deploying and using data-driven technologies, to ensure they abide by the ethical principles for data initiatives developed by the Nuffield Council on Bioethics. One of the code’s principles requires organisations to "explain algorithms to those taking actions based on their outputs" and "undertake ethical examination of data use specific to this use-case". | 19 February 2019  | Code of conduct |
| Information Commissioner’s Office (ICO) news: February 2019 | The ICO has been working on a number of initiatives, including:  

- The ICO and Financial Conduct Authority (FCA) have signed a memorandum of understanding establishing a framework for cooperation, coordination and information sharing.  
- The ICO is focussing on the world of ad-tech, programmatic advertising and real-time bidding (in line with their Tech Strategy), and both online tracking and artificial intelligence are priority areas. They have identified three main areas of interest: transparency, lawful basis for processing and security.  
- **Criminal prosecution/ fine for ignoring a DSAR** – The ICO has reminded organisations that they could face criminal prosecution if they | February 2019  | ICO and FCA memorandum of understanding  
Ad-tech commentary  
DSAR prosecution news  
Data protection fee blog post  
Regulatory sandbox discussion paper |
### United Kingdom

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Development</strong></td>
<td><strong>Summary</strong></td>
<td><strong>Impact date</strong></td>
<td><strong>Links</strong></td>
</tr>
<tr>
<td></td>
<td>fail to respect people’s right to access their personal information, by reporting that a housing developer was fined £300 by Westminster Magistrates for ignoring a DSAR (under the DPA 1998 regime).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- ICO blogs on non-payment of data protection fees</td>
<td>The blog post explains why small businesses need to pay the data protection fee.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Regulatory sandbox</td>
<td>The ICO has published a discussion paper on their sandbox initiative. The purposes of the sandbox are: (1) to support the use of personal data in innovative products and services that can be shown to be in the public interest; (2) to help develop a shared understanding of what compliance in particular innovative areas looks like; and (3) to support the UK in its ambition to be an innovative economy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Council officer fined for disclosing recruitment data</td>
<td>A senior council officer was prosecuted for disclosing personal information of rival job applicants (including CVs) to his partner.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Phone-paid Services Authority (PSA) has launched a consultation on draft guidance aimed to clarify the PSA’s expectations for the retention period of certain types of relevant data. The proposals for the guidance are aimed to support the PSA’s access to such data in the event of an investigation into a service provider. The closing date for responses is 3 April 2019.</td>
<td>3 April 2019 (consultation closes)</td>
<td>Consultation</td>
</tr>
<tr>
<td></td>
<td>The Investigatory Powers Commissioner’s Office (IPCO) published their first annual report on the use of investigatory powers during 2017. The report is a comprehensive account of the oversight work carried out by IPCO and their predecessor organisations (the Office of the Surveillance Commissioners, the Interception of Communications Commissioner’s Office and the Intelligence Service Commissioner.</td>
<td>31 January 2019</td>
<td>IPCO annual report Press statement</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>No deal Brexit: SIs published this month</td>
<td>The Electronic Communications (Amendment etc.) (EU Exit) Regulations 2019 amend legislation relating to the notification of personal data breaches by providers of electronic communications services (including Directive 2002/58/EC and Commission Regulation (EU) 611/2013), and revoke direct EU legislation which is redundant or otherwise inappropriate to retain on the UK’s statute book after exit from the EU.</td>
<td>Exit day (UK leaves the EU)</td>
<td>Electronic Communications (Amendment etc.) (EU Exit) Regulations 2019</td>
</tr>
<tr>
<td>New guidance for local authorities on the flow of personal data from the UK to the EEA</td>
<td>The government has published new guidance for local authorities on the flow of personal data from the UK to the EEA that collates stakeholder and sector guidance on Brexit, focusing on preparing for the no-deal Brexit scenario.</td>
<td>Exit day (UK leaves the EU)</td>
<td>Guidance</td>
</tr>
<tr>
<td>National Data Guardian empowered to publish guidance on processing of health and social care data</td>
<td>The Health and Social Care (National Data Guardian) Act 2018 (Commencement) Regulations 2019 were made on 14 March 2019, and they will bring the Health and Social Care (National Data Guardian) Act 2018 (HSCNDGA 2018) into force on 1 April 2019. The HSCNDGA 2018 empowers the National Data Guardian for Health and Social Care (Data Guardian) to publish guidance about the processing of health and adult social care data in England.</td>
<td>1 April 2019</td>
<td>Regulations</td>
</tr>
<tr>
<td>ICO adtech developments</td>
<td>The Information Commissioner’s Office (ICO) commissioned research which has been published in partnership with Ofcom as a very interesting report on consumers’ attitudes towards and awareness of personal data used in online advertising. According to Ofcom: “Advertising technology – known as “adtech” – refers to the different types of analytics and digital tools used to direct online advertising to individual people and audiences. It relies on collecting information about how individuals use the internet, such as search and browsing histories, and personal information, such as gender and year of birth, to decide which specific adverts are presented to a particular person. Websites also use adtech to sell advertising space in real-time.” The research finds that 54% of participants would rather see relevant online adverts. But while 63% of people initially thought it acceptable for websites to display adverts, in return for the website being free to access, this fell to 36% once it was explained how personal data might be used to target adverts. The ICO also published a summary report of their Adtech Fact Finding Forum held on 6 March.</td>
<td>March 2019 and ongoing</td>
<td>ICO and Ofcom report Adtech Fact Finding Forum summary report</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>ICO calls for participants in the development of its auditing framework for AI</td>
<td>Simon McDougall (ICO’s Executive Director for Technology Policy and Innovation) announced that the ICO will be developing a framework for auditing the use of personal data in artificial intelligence (AI) and invited organisations to participate in the development process. In addition to its audit function, the framework will also provide guidance to assist organisations develop and apply AI in compliance with data protection law, including information on assessing and managing the data protection risks of AI applications. The ICO expects to publish a formal consultation paper on the subject by January 2020 and the final AI auditing framework and associated guidance to be published by spring 2020.</td>
<td>Ongoing</td>
<td><a href="#">Blog post</a></td>
</tr>
<tr>
<td>Court of Appeal holds that Government’s collection and storage of data from an individual’s public statements did not infringe privacy</td>
<td>In <em>R (Butt) v Secretary of State for the Home Department [2019] EWCA Civ 256</em>, the court agreed that the Government’s collection and storage of data from an individual’s public statements did not infringe privacy and did not constitute unauthorised covert directed surveillance under the Regulation of Investigatory Powers Act 2000.</td>
<td>8 March 2019</td>
<td><a href="#">Judgment</a></td>
</tr>
<tr>
<td>ICO conducts raids on businesses suspected of making nuisance calls</td>
<td>The ICO searched two addresses as part of an investigation into businesses suspected of making live and automated nuisance calls. Following a year-long investigation, two teams of ICO enforcement officers executed search warrants at offices in Brighton and Birmingham. The businesses are suspected of making millions of calls to UK landline and mobile numbers. The ICO has received nearly 600 complaints about the businesses. The calls mainly concerned road traffic accidents, personal injury claims, and insurance for household goods. People who received the calls were unable to identify who the calls were from or opt out of them.</td>
<td>12 March 2019</td>
<td><a href="#">Press statement</a></td>
</tr>
<tr>
<td>Two Birmingham workers fined for data protection breaches</td>
<td>Two workers in Birmingham were prosecuted for breaching the Data Protection Act 1998 by unlawfully obtaining personal data – in one case by accessing certain personal data without a business need to do so, and in another case for forwarding work email containing customer and staff personal data to a personal email account.</td>
<td>18 March 2019</td>
<td><a href="#">Press statement</a></td>
</tr>
<tr>
<td>FCA publication provides insights on cyber resilience good practice</td>
<td>The FCA has published a document bringing together industry insights on cyber resilience. Part of the FCA’s role is to help firms become more resilient to cyber-attacks, so reducing the risk and frequency of disruption. The FCA says the publication may be particularly relevant for small and medium-sized firms, but encourages all firms to consider whether these insights may be useful to them.</td>
<td>8 March 2019</td>
<td><a href="#">Report</a></td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Government “Cyber Governance Health Check” report</td>
<td>The Government’s 2018 “Cyber Governance Health Check” report examines the UK’s FTSE 350 companies’ approach to cybersecurity and found that boards at many of those companies still haven’t grasped the severity of the impact that a cyber-attack can have on their business.</td>
<td>March 2019</td>
<td>Report</td>
</tr>
<tr>
<td>Public authorities compliance with consultation requirements under GDPR</td>
<td>DCMS has released guidance to help public authorities comply with Article 36(4) GDPR (the requirement for public authorities in the UK to consult with the ICO on any proposals for legislative or statutory measures they are developing which involve the processing of personal data).</td>
<td>26 February 2019</td>
<td>Guidance</td>
</tr>
<tr>
<td>Investigation into bias in the use of algorithms in criminal justice</td>
<td>The Centre for Data Ethics and Innovation will be partnering with the Cabinet Office’s Racial Disparity Unit to explore the potential for bias in the use of algorithms in crime and justice, financial services, recruitment and local government.</td>
<td>Ongoing</td>
<td>Press statement</td>
</tr>
<tr>
<td>New artificial intelligence advisory committee</td>
<td>Lord Burnett of Maldon, the current Lord Chief Justice, has set up a new AI Advisory to provide the senior judiciary with guidance on: (i) the likely impact of developments in AI on the Judiciary and the court system; (ii) ways of ensuring that judges are sufficiently trained on AI and its impact; and (iii) the most pressing legal, ethical, policy, cultural and economic effects of AI.</td>
<td>Ongoing</td>
<td>Press statement</td>
</tr>
</tbody>
</table>
United Kingdom
## Development

### Provisions on the Administration of Blockchain Information Services (Blockchain Provisions)

The aim of the Blockchain Provisions is to regulate blockchain information service activities within the PRC. It defines blockchain information services as "information services provided to the public in such forms as Internet websites and application programs based on blockchain technologies or systems" and identifies blockchain information service providers as subjects or nodes that provide blockchain information services to the public and the institutions or organizations that provide technical support to such subjects.

The Blockchain Provisions also specify the requirements that must be satisfied for blockchain information service providers to provide services to users such as identity verification and for new services/functions and products to be submitted to the relevant cyber administration for security assessment.

- **Impact date**: 15 February 2019
- **Links**: Link (Chinese)

### Information Security Technology – Personal Information Security Specification (Draft) (Draft Specification)

The Draft Specification updates the previous Personal Information Security Specification which took effect in 1 May 2018 and further restricts certain areas of personal data collection. This includes prohibiting the bundling of consent authorisation for personal data collection and establishes rules in the context of third party personal data collection.

The Draft Specification also specifically identifies and tackles situations where elements of coercion is used such as prohibiting personal data collecting parties from lowering service quality or restricting functionalities if an individual refuses to consent to personal data collection.

- **Impact date**: 1 February 2019 (Published)
- **Links**: Link (Chinese)
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules on the Administration of Mobile Internet Application (App) Security Verification Implementation (App Rules)</td>
<td>The App Rules provide for the assessment and verification of the personal data collection features and functionalities of mobile internet applications in the People’s Republic of China, setting out the following procedure for certification and post-certification regulation: (i) technical verification by a recognised testing institution; (ii) on-site verification by the certification authority; and (iii) continuing post-certification regulation by the certification authority (either on a daily basis or a targeted review when personal data breaches arise). The App Rules also specify circumstances when app creators are disqualified from applying for certification, such as non-compliance with applicable laws and regulations and when major personal data security breaches have occurred within the past twelve months.</td>
<td>15 March 2019</td>
<td>Link (Chinese)</td>
</tr>
</tbody>
</table>
**Development**

Government highlights the need to improve law enforcement and the judiciary in the investigation and prosecution of cybercrime

**Summary**

A three-day workshop on Cybersecurity Capacity Assessment and Cybersecurity Capacity Maturity Model for Nations was organised by the Mauritian Ministry of Technology, Communication and Innovation in collaboration with the World Bank and the University of Oxford.

The aim of the workshop was to increase the scale and effectiveness of cybersecurity capacity-building, by gaining a more comprehensive understanding and review of the current national cybersecurity capacity landscape.

The Government of Mauritius highlighted that this understanding and review is important, in view of the considerable changes in the cybersecurity landscape of Mauritius. The necessity to improve law enforcement as well as the judiciary in the investigation and prosecution of cybercrime as well as the enhancement of safety and security in cyberspace, while also respecting core human rights’ values and interests, such as privacy and freedom of expression, are measures which the Mauritian Government intends to adopt.

**Impact date**: 13-15 February 2019

**Links**: [Cybersecurity Capacity Maturity Model Workshop](#)

---

Mauritius becomes the first jurisdiction to offer a regulatory framework for the custody of Digital Assets as from 1 March 2019

**Summary**

Following consultations and discussions with the Organisation for Economic Cooperation and Development on the governance and regulation of digital financial assets, the Mauritius Financial Services Commission (FSC) has implemented rules for the grant of Custodian Services (Digital Asset) Licences, effective as of 1 March 2019.

Through the implementation of this regulatory framework, Mauritius positions itself as the first jurisdiction globally to offer a regulated landscape for the custody of digital assets.

These rules shall apply to any person carrying out custodian services for digital asset and whose objects shall be limited to the safe-keeping of the digital asset and operations arising directly from it.

**Impact date**: 1 March 2019

**Links**: [Financial Services (Custodian Services (Digital Asset)) Rules 2019](#)
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>After local recognition of Digital Assets as an asset-class for investment by Sophisticated and Expert Investors in September 2018, these new rules bring the Mauritius International Financial Centre a step closer to its objective of becoming the FinTech hub, in and for, Africa.</td>
<td></td>
<td></td>
<td>5th Annual (SIL) e-Gov Conference on AI and Blockchain</td>
</tr>
<tr>
<td>Government’s wishes to apply AI and Blockchain technologies for a more effective public service delivery</td>
<td>During the 5th Edition of the Annual (State Informatics Ltd) e-Gov conference, aimed at sharing new technological trends that affect governments around the world with regards to artificial intelligence and blockchain, the Government of Mauritius emphasised on its continuous efforts to promote innovation and new technologies as essential tools for an effective public service delivery. Among the intended initiatives of the Government of Mauritius is the digital transformation of the procedures at the National Transport Authority (NTA) for the registration of vehicles, by using blockchain technology. Historically criticised for its cumbersome procedures in place, the NTA may well become the first public service organisation in Mauritius to adopt such technology.</td>
<td>28 March 2019</td>
<td>5th Annual (SIL) e-Gov Conference on AI and Blockchain</td>
</tr>
</tbody>
</table>
## United States

### Contributors

**Michael Bahar**  
Partner  
**T:** +1 202.383.0882  
michaelbahar@eversheds-sutherland.com

**Ali Jessani**  
Associate  
**T:** +1 202.383.0950  
alijessani@eversheds-sutherland.com

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NFA Amends Interpretive Notice Regarding Cybersecurity Information Systems Security Program</strong></td>
<td>On 7 January, the National Futures Industry (NFA) amended its interpretive notice regarding cybersecurity. The amendments, set to go into effect on 1 April 2019, will update the current Information Systems Security Program (ISSP) requirements that NFA members have to comply with in three important ways. First, the amendments require members to provide cybersecurity training to employees at least annually and more frequently if warranted, in addition to training upon hiring as is currently required. Second, the amendment clarifies the appropriate officers that may approve the ISSPs. Finally, and perhaps most importantly, the amendment to the interpretive notice requires members to notify the NFA of a security incident in certain circumstances. The rule does not yet specify how long companies will have to make the notification.</td>
<td>1 April 2019</td>
<td>NFA Amendment</td>
</tr>
</tbody>
</table>
| **Massachusetts Updates Data Breach Notification Law** | On 10 January, Massachusetts Governor Charlie Baker signed a bill amending the state's data breach notification requirement. Set to go into effect on 11 April 2019, the amendments will require:  
1) Companies that suffer data breaches involving social security numbers to provide credit monitoring services for 18 months to affected consumers free of charge; this requirement is 42 months if the company that suffered the breach is a credit monitoring agency;  
2) Post-breach notice sent to the Massachusetts Attorney General and the state’s Office of Consumer Affairs and Business Regulation (OCABR) to include whether the company has a written information security program in place and the type of information compromised; and  
3) Corporations providing post-breach notification to consumers to identify any parent or affiliated corporations. | 11 April 2019 | H. 4806 |
### Development Summary

These amendments will make Massachusetts’ data breach notification laws one of the more onerous in the country.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illinois Supreme Court Finds that Plaintiffs Need Not Show Actual Harm under BIPA</td>
<td>In a unanimous decision on 25 January 2019, the Illinois Supreme Court found that a plaintiff need not show actual harm to seek relief under the state’s Biometric Information and Privacy Act (BIPA). Instead, the court held that a procedural harm is sufficient to bring forth a claim under the law. This will likely open up the floodgates in terms of the lawsuits brought under BIPA.</td>
<td>25 January 2019</td>
<td>Rosenbach v. Six Flags Entertainment Corp.</td>
</tr>
<tr>
<td>US District Court Dismisses Vast Majority of Claims against CareFirst</td>
<td>On 30 January, DC District Court Judge Christopher R. Cooper, in Attias v Carefirst, Inc., agreed with Eversheds Sutherland attorneys Matt Gatewood and Robert Owen when he dismissed the vast majority of claims against the health insurer. Judge Cooper held that while plaintiffs’ “alleged injuries may be enough to establish standing at the pleading stage of the case, they are largely insufficient to satisfy the ‘actual damages’ element of nine of their state-law causes of action.” He concluded that the Complaint’s allegations of future risk of identity theft, loss of the benefit of the bargain, prophylactic purchase of credit monitoring, and emotional distress were not enough to clear the requirement that actual damages be stated.</td>
<td>29 January 2019</td>
<td>Attias v. Carefirst, Inc.</td>
</tr>
<tr>
<td>Deadline Passes in California Assembly to Introduce Bills Amending CCPA</td>
<td>22 February marked the last day that new bills could be introduced in the California Assembly. There were a number of proposals introduced before or on this date to amend the impending California Consumer Privacy Act (CCPA). Most notable is SB-561, which would expand the private right of action under the CCPA to all violations of consumer rights. Currently, the law only allows for a private right of action if a consumer’s personal information is subject to a data breach as a result of a business failing to maintain reasonable security procedures. The CCPA is still set to go into effect on 1 January 2020.</td>
<td>1 January 2020</td>
<td>SB-561</td>
</tr>
<tr>
<td>FTC Issues Largest Fine Ever Under COPPA</td>
<td>On 27 February, the Federal Trade Commission announced a settlement with video social networking app TikTok, in which the company agreed to pay $5.7 million for violating the Children’s Online Privacy Protection Act (COPPA), the largest fine issued under the law to date. According to the FTC, the company was aware that children under 13 were using the app but failed to obtain parental consent prior to collecting the children’s names, email addresses, and phone numbers, among other information. The FTC also alleged the company failed to inform parents of its information collection practices and delete children’s collected personal information upon request by their parents. Along</td>
<td>27 February 2019</td>
<td>FTC Press statement</td>
</tr>
</tbody>
</table>
### Development

<table>
<thead>
<tr>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>with the penalty, the FTC’s settlement requires the company’s information collection practices to be in compliance with COPPA going forward.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDYFS Third-Party Service Provider Requirement Goes Into Effect</td>
<td>1 March 2019</td>
<td><a href="#">23 NYCFR 500</a></td>
</tr>
<tr>
<td>As of 1 March 2019, the New York State Department of Financial Services’ (NYDFS) cybersecurity regulation, 23 NYCRR Part 500, requires financial services institutions regulated by NYDFS to implement policies and procedures to address the cybersecurity risks posed by third-party service providers to the institutions’ nonpublic information (NPI). To manage the risks and potential liability that come with this “first of its kind” cyber regulation, covered entities must implement an ongoing program that in most cases will reflect a sea change from their prior practices. In particular, the required oversight and management of third-party service providers, or TPSPs, will expand well beyond traditional vendor management functions and deep into contracting, diligence and stakeholder review.</td>
<td></td>
<td><a href="#">Article on Legal Tech News</a></td>
</tr>
<tr>
<td>FTC Proposes Amendments to Safeguards and Privacy Rule under Gramm-Leach-Bliley Act</td>
<td>5 March 2019</td>
<td><a href="#">FTC Press statement</a></td>
</tr>
<tr>
<td>On 5 March 2019, the FTC announced that it was seeking comments regarding proposed changes to the Safeguards Rule and the Privacy Rule under the Gramm-Leach-Bliley Act (GLBA). Among other changes, the FTC is proposing more detailed requirements for what companies need to include in the information security plan required under the Safeguards Rule. The proposed rule would alter existing requirements of an information security program and add several new elements. For example, the current rule states requires covered entities to designate “an employee or employees to coordinate [their] information security program.” The amended rule would require the designation of a single qualified individual (the Chief Information Security Officer) responsible for overseeing the information security program. The amended rule would further require financial institutions to restrict access to physical locations containing customer information only to authorized individuals. The rule would also expand the definition of “financial institution” under both the Safeguards Rule and Privacy Rule to include those individuals who charge a fee to connect consumers who are looking for a loan from a lender. The rule otherwise rejects calls to add more specificity to what companies need to do to safeguard non-public personal information. Instead, it states that security is not a “check the box” exercise, especially in light of changing technology and changing threats. Comments must be made within 60 days of when the rule was published in the federal register.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Washington State Senate Passes its Version of the GDPR</td>
<td>On 6 March 2019, Washington state’s senate passed a comprehensive data privacy bill that more closely mirrors the GDPR than does California’s 2018 Consumer Privacy Act, but contains many of the same obligations on companies. Among other things, it would create enhanced transparency requirements and would allow consumers to access what data companies collect; correct inaccurate data; and oblige companies to delete consumer data under certain conditions. The law also requires companies using facial recognition technology for profiling to employ meaningful human review prior to making final decisions based on such profiling where such final decisions product legal effects and to obtain consumer consent prior to deploying facial recognition services in physical premises open to the public. The bill still needs to be reconciled with the Washington State’s House version of the bill, and then signed by the Washington Governor, before it can become law. Recent developments indicate that it will not pass into law in 2019, but that could still change.</td>
<td>6 March 2019</td>
</tr>
</tbody>
</table>
# Russia

## Contributors

**Ivan Kaisarov**  
Associate  
**T:** +7 812 363 3377  
ivan.kaisarov@eversheds-sutherland.ru

**Ekaterina Mironova**  
Senior Associate  
**T:** +7 495 662 6434  
ekaterina.mironova@eversheds-sutherland.ru

**Victoria Goldman**  
Managing Partner  
**T:** +7 812 363 3377  
victoria.goldman@eversheds-sutherland.ru

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
</table>
| Inspections of personal data operators | The Russian government has approved new rules (which came into force on 23 February 2019 and replaced prior regulations), according to which the Federal Service for the Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) will conduct inspections of personal data operators. Overall, the new provisions are more detailed and provide more predictability for individuals and businesses. Under the new rules, routine inspections can be carried out, but only once three years has passed after:  
- the personal data operator officially registered as a company or as an individual entrepreneur; or  
- the end of the last scheduled inspection of the personal data operator. However, the rule above does not apply to the following personal data operators, which can be inspected every two years:  
- personal data operators which collect biometric personal data and special categories of personal data (data on ethnicity, political views, religious or philosophical beliefs, health, intimate life);  
- personal data operators which transfer personal data to foreign countries which do not provide an adequate level of data protection (for example the USA); or | 23 February 2019 | Inspections of personal data operators |

---

*Updata Edition 3 - January to March 2019 | Updates by territory*
Russian companies that are processing personal data on behalf of a foreign company that is not registered in Russia.

Previously, inspections, whether scheduled or unannounced, could be both on-site inspections or document-based inspections. Under the new rules, unscheduled document-based inspections will no longer be performed. For a document-based check, which can now only be carried out as part of a scheduled inspection, the deadline for submitting documents to Roskomnadzor is reduced (from ten to five business days), as is the deadline for submitting explanations related to any inconsistency in the information provided (three business days instead of ten).

The Russian government has introduced a new legal basis to initiate unannounced inspections, namely by decision of the head of Roskomnadzor (or any of its regional branches). The decision must nevertheless be based on violations that were identified through the daily monitoring of personal data operator’s activity. This provision provides Roskomnadzor with extensive discretionary powers to perform unscheduled inspections. However, the duration of such inspections is now halved compared to the older rules (ten business days instead of twenty).

In addition, the new regulation introduces a rather long list of grounds for extending the period of inspection. Previously, the duration of the inspection could be increased only if it required complex investigations. Now, other grounds can be invoked by the regulator, such as the operator’s failure to submit necessary documents, if a law-enforcement agency transmits evidence indicating violations of data protection rules, or if unforeseen circumstances have occurred.

The new regulation also introduces a deadline of six months for remediying violations of data protection rules. The previous regulation did not provide such a deadline.

Updating the list of countries which provide an adequate level of data protection

Russian law applies more lenient rules for cross-border transfers of personal data when the data is sent to:

- foreign countries which have ratified the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108); or
- foreign countries which provide an adequate level of data protection according to Roskomnadzor.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updating the list of countries which provide an adequate level of data protection</td>
<td>Russian law applies more lenient rules for cross-border transfers of personal data when the data is sent to:</td>
<td>16 February 2019</td>
<td>Publication on the official website</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Impact date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>The list of countries which provide an adequate level of data protection was recently updated by Roskomnadzor. Japan was added to this list, and therefore the transfer of personal data to Japan no longer requires specific written consent from the personal data subject.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Development

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Impact date</th>
<th>Links</th>
</tr>
</thead>
</table>
| **Onshore Dubai – Smart Dubai AI Ethics Guidelines** | The technology arm of the Dubai government, known as Smart Dubai, has published a new Ethical AI Toolkit. The Toolkit includes:  
- a comprehensive document setting out the overarching principles of ethical AI accompanied by a set of guidelines that expand on the ethical principles and provide practical examples; and  
- a Self-Assessment Tool that allows AI developers and operators to evaluate the ethical level of their AI systems.  
Smart Dubai, together with its AI Ethics advisory board, are currently reviewing the legal framework to support the implementation of ethical AI across the emirate of Dubai. | 8 January 2019 | Press statement |
| **DIFC - Data Protection Policy Guidance published** | The Commissioner of Data Protection in the DIFC published policy guidance on direct marketing and electronic communications.  
The guidance note covers all personal data processed for electronic direct marketing purposes and includes a helpful Do's and Don'ts section. | 10 January 2019 | Guidance |
| **Federal – New law on IT and data protection for healthcare sector** | UAE Federal Law No. 2 of 2019 regarding the use of information and communication technology in the healthcare sector (Healthcare IT Law) is expected to come into force in May of this year.  
The law will be the first federal law to specifically address data and privacy issues in the UAE, albeit it is limited to the Healthcare sector. For more information, see our Spotlight on... briefing. | TBC | Eversheds Sutherland briefing |
Spotlight on…

- **Irish Data Protection Commission publishes first annual report since GDPR**
  We examine the Irish Data Protection Commissioner’s first annual report since the introduction of GDPR on 25 May 2018. Read more...

- **Romanian implementation of the GDPR**
  We report on Romania’s recently introduced data protection law, focussing on the provisions relating to the processing of national identification numbers and the rules on the use of CCTV and monitoring in an employment context. Read more...

- **Court action: a strategic option for data security breach response – a UK perspective**
  We consider various options offered by UK Courts which can help companies take action against the perpetrators of cyber attacks. Read more...

- **UK’s Privacy and Electronic Communications (Amendment) Regulations 2018**
  We consider the impact of the recently passed Privacy and Electronic Communications (Amendment) Regulations 2018, which empowered the ICO to issue to directors and other company officers for breaches of the rules governing electronic direct marketing communications. Read more...

- **Organisations in the UAE prepare for new Healthcare IT Law**
  We explore the UAE’s impending Healthcare IT Law – the first federal law to address privacy issues within the context of data processing in the UAE (albeit limited to the healthcare sector) which will introduce new obligations for entities in the healthcare sector. Read more...

- **Data Protection and Brexit – what you can do to prepare**
  We set out the key actions that businesses can take to help prepare for a “no deal” Brexit. Read more...

- **The "transfers from EU back into the UK conundrum"**
  We discuss the issue of EU-based processors ensuring lawful transfers back to the UK. Read more here (Part 1) and here (Part 2)
For further information, please contact:

**Paula Barrett**  
Co-Lead of Global Cybersecurity and Data Privacy  
**T:** +44 20 7919 4634  
paulabarrett@eversheds-sutherland.com

**Michael Bahar**  
Co-Lead of Global Cybersecurity and Data Privacy  
**T:** +1.202.383.0882  
michaelbahar@eversheds-sutherland.us

**Lizzie Charlton**  
Data Privacy Professional Support Lawyer  
**T:** +44 20 7919 0826  
lizziecharlton@eversheds-sutherland.com

@ESPrivacyLaw

eversheds-sutherland.com

© Eversheds Sutherland 2019. All rights reserved.  
Eversheds Sutherland (International) LLP and Eversheds Sutherland (US) LLP are part of a global legal practice, operating through various separate and distinct legal entities, under Eversheds Sutherland. For a full description of the structure and a list of offices, please visit www.eversheds-sutherland.com.  
This information is for guidance only and should not be regarded as a substitute for research or taking legal advice.