Update
Your quarterly Data Privacy and Cybersecurity update

July to September 2020
Welcome to the ninth edition of Updata!

Updata is an international report produced by Eversheds Sutherland’s dedicated Privacy and Cybersecurity team – it provides you with a compilation of key privacy and cybersecurity regulatory and legal developments from the past quarter.

This edition covers July to September 2020 and is full of newsworthy items from our team members around the globe, including:

- not surprisingly, the Schrems II court decision which invalidated the EU-US Privacy Shield and requires additional due diligence before using the Standard Contractual Clauses, dominates. There are indications that the EU and US will work towards a new Privacy Shield framework and some data protection authorities (particularly in Germany) have published guidance following the Schrems II decision. In Austria Max Schrems’ NGO filed complaints against a large number of websites following Schrems II although the Austrian Courts denied most of his previous claim against Facebook;
- the data privacy ramifications of COVID-19 continue to develop, with a new Teleworking Law in Spain, and in Germany the Data Protection Conference discussed the use of imaging cameras or electronic temperature recording in the context of COVID-19;
- new laws have been published in Switzerland (finally!) and China (draft);
- in the UK, recent statements have cast doubts as to whether any post-Brexit adequacy decision will be reached between the EU and the UK;
- significant enforcement action against telecommunications operators has taken place in Italy, and in France the CNIL has published a whitepaper on voice assistants; and
- in the USA, changes have been made to data breach notification laws in Indiana, Louisiana and Virginia; while the California legislature has allowed businesses at least another year to expand their privacy programmes to cover B2B and employee information.

We hope you enjoy reading this edition.

Follow us on Twitter at:

@ESPrivacyLaw

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.com
## Development

| Transfers of data from the EU to the US: CJEU strikes down EU-US Privacy Shield Framework in Schrems II decision |

The Court of Justice of the European Union ("CJEU") issued its highly anticipated decision regarding the validity of the EU-US Privacy Shield Framework for personal data transfers (Case C-311/18) between the EU and the US.

The decision, widely known as the Schrems II case, stated that the current Privacy Shield arrangements do not adequately protect individual data rights in the EU when personal data is transferred to the US pursuant to the Privacy Shield Framework. Following the CJEU decision, the Privacy Shield is invalid and can no longer be used for transfers of personal data from the EU to the US.

By way of background to this case, Max Schrems challenged the legal basis upon which Facebook Ireland relied in respect of the transfer his personal data from the EU to the US in a complaint to the Irish Data Protection Commissioner in 2015. The Irish High Court which subsequently received the complaint, referred several questions to CJEU which included queries relating to the legality of the Standard Contractual Clauses ("SCCs") and EU-US Privacy Shield as adequate mechanisms for international transfers of personal data.

In its ruling, the CJEU decided that the Privacy Shield was invalid on two grounds:

- US surveillance programs are not constrained to processing data which is strictly necessary and proportionate and therefore do not comply with Article 52(1) of the EU Charter on Fundamental Rights ("EU Charter"); and

<table>
<thead>
<tr>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 July 2020</td>
<td>ES Statement</td>
</tr>
</tbody>
</table>
EU citizens do not have effective means of redress in the US in the event of unlawful surveillance under the Privacy Shield framework, as required by Article 47 of the EU Charter. However, as mentioned above, the CJEU’s decision was not solely focused on the Privacy Shield – it further considered the validity of the SCCs as a mechanism for the export of personal data pursuant to Article 46 of the GDPR (appropriate safeguards).

Whilst the SCCs remain a valid data transfer mechanism, the CJEU’s decision casted doubt on practical implementation going forward. Companies, usually as controllers, will be required to conduct a case-by-case assessment on whether the circumstances of the transfer of personal data provide adequate protection and meet EU requirements (i.e. it is not enough that the data exporter and importer enter into SCCs; a case-by-case assessment of whether the importer can comply with the provisions of the SCCs is necessary). This means that, where necessary, companies are required to offer additional safeguards in addition to the SCCs.

In its judgment, the CJEU emphasised existing SCCs Clauses 5, 6 and 12 which provide (i) that where the recipient of data in a third country cannot adequately protect EU personal data, it must return or destroy the data received and (ii) that a resulting right arises for the data subject to receive compensation for damage suffered. As explained in other updates below, some data protection authorities have issued guidance in relation to this.

### European Commission releases statements on Schrems II case

The Vice-President of the European Commission for Values and Transparency and the Commissioner for Justice have issued joint statements on the Schrems II judgment.

Vice-President Jourová welcomed the Schrems II decision as confirmation that the protection of European Citizens’ data is absolutely fundamental. To support this, Vice-President Jourová stated that it is important to have a broad toolbox for international data transfers which can ensure a high level of data protection. In addition, Vice-President Jourová confirmed that the European Commission would be working more closely with its American counterparts to ensure safe transatlantic data transfers. Commissioner Reynders also welcomed the Schrems II decision.
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDPB issues FAQs on implications of the Schrems II case</td>
<td>The European Data Protection Board (&quot;EDPB&quot;) has issued FAQs on the invalidation of the Privacy Shield and the implications for the SCCs, in the wake of the Schrems II judgment. Amongst other things, the FAQs make clear that (i) there is no grace period during which Privacy Shield can still be relied upon; and (ii) the elements of the judgment which relate to SCCs are (a) also relevant to Binding Corporate Rules (&quot;BCRs&quot;) and (b) are not just limited to application to transfers to the US (i.e. the judgment applies to transfers of personal data pursuant to SCCs in respect of any third country).</td>
<td>23 July 2020</td>
<td>EDPB FAQs</td>
</tr>
</tbody>
</table>
| EU and US issue joint statement on new Privacy Shield framework | The European Commission and the US Department of Commerce have issued a joint statement confirming that they have commenced discussions to establish a new EU-US Privacy Shield framework to comply with the Schrems II decision. Both parties acknowledged the importance of data protection in transatlantic transfers of personal data and have a stated shared commitment to secure fundamental rights and uphold the rule of law. | 10 August 2020 | Joint statement - Commission  
Joint statement - US |
| EDPB creates task forces in aftermath of the Schrems II judgment | The EDPB has created two task forces in the light of Schrems II to:  
- review various complaints received; and  
- prepare recommendations to assist controllers and processors to meet their duty to identify and implement supplementary measures to protect personal data when transferring it to third countries. | 4 September 2020 | Press release |
| European Parliament publishes Paper summarising Schrems II and its implications | The European Parliament has published a paper in which it summarises the outcome of the CJEU judgment in Schrems II. The paper also explores the implications of the judgment as well as first reactions by commentators and data protection authorities. | 15 September 2020 | Paper |
| New legal solution proposed for transfers of personal data outside the EU following Schrems II | The EU Cloud Code of Conduct Assembly (the “Assembly”), which consists of cloud service providers ("CSPs") and small and | 15 September 2020 | Press release |
medium-sized companies, has announced that a proposed legal solution is currently being developed which would facilitate the transfer of personal data outside the EU in the wake of the *Schrems II* decision.

If approved by data protection authorities, this solution could be an alternative to the EU-US Privacy Shield, following *Schrems II*. The Assembly has invited interested CSPs and cloud-users to contribute to the development of the proposal.

### IAB Europe issues FAQs on the impact of Schrems II on online advertising

The Interactive Advertising Bureau ("IAB") has issued a list of frequently asked questions (the "FAQs") following the *Schrems II* decision.

Specifically, the FAQs summarise the impact of *Schrems II* on the online advertising industry, highlight pitfalls to avoid and set out where to seek detailed guidance. Additionally, the IAB notes that the *Schrems II* decision will likely result in a significant disruption to the online advertising industry, taking into account the industry's global and interconnected nature.

### European Commission highlights importance of data sharing to defeat Covid-19

The European Commission has highlighted the importance of sharing health data more freely across the EU in the fight against COVID-19. Data sharing is crucial to understanding and being able to manage the virus; it has helped scientists to track how the virus spreads, and enabled doctors to effectively identify symptoms of the virus and share methods of treatment. Other parties such as pharmaceutical companies and researchers have also been able to use data relating to the virus and patient immune responses to expedite the development of potential vaccines and treatments.

However, it remains important to consider individuals' privacy when sharing health data, as much of this data contains personal and sensitive details about patients. The Commission has therefore acknowledged that sharing of such data should only take place where the privacy of patient's data is guaranteed, which it says may be facilitated by projects such as MyHealthMyData and SHiELD.
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>European Commission’s new Implementing Decision to enhance contact-tracing technology</strong></td>
<td>The European Commission has decided to adopt a new Implementing Decision which would establish a &quot;voluntary gateway service&quot; to improve the interoperability of contact-tracing and warning mobile apps. This service intends to build on the interoperability guidelines, technical specifications agreed by the Member States, the principles of the EU toolbox and EU guidelines on data protection for mobile applications. For example, it allows for the sharing of pseudonymised information obtained by national contact-tracing apps in a safe way between Member States.</td>
<td>15 July 2020</td>
<td>Press release</td>
</tr>
</tbody>
</table>
| **Testing underway for European Commission’s new interoperability gateway service to link national contact tracing apps** | The European Commission has announced that a group of EU member states (the Czech Republic, Denmark, Germany, Ireland, Italy and Latvia) has started testing the Commission’s new interoperability gateway service for contact tracing and warning apps.  

The service links national coronavirus contact tracing and warning apps across the EU in order to facilitate the management and containment of coronavirus outbreaks and break the transmission chain of the virus.  

Using one app, users will be able to report test results or receive alerts, even if they travel abroad. The gateway will exchange minimised, encrypted and pseudonymised data, which will only be retained for the period required for tracing purposes.  

The Commission reports that, after testing, the service will start to be operational in October. | 14 September 2020 | Press release          |
| **EDPS issues advice to EU institutions and authorities on body temperature checks** | The European Data Protection Supervisor ("EDPS") has issued advice to EU institutions, bodies, offices and agencies ("EUIs") about the use of body temperature checks in the fight against COVID-19.  

The EDPS commented that some use of temperature checks risks violating individuals’ privacy and has advised EUIs to collect only the minimum amount of data required. The EDPS also commented that body temperature checks carried out on a mandatory basis should not be solely undertaken by software, but should be supplemented by human intervention. In addition, and given the ever-changing nature of the pandemic, the necessity | 1 September 2020               | Press release          |
and proportionality of use of temperature checks should be kept under constant review.
Although directed at EUIs, the guidance provides some insight into the EU's approach to privacy in the context of the ongoing COVID-19 pandemic.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection authorities write open letter to video teleconferencing</td>
<td>Data protection authorities in the United Kingdom, Canada, Switzerland, Hong Kong, Gibraltar and Australia have come together to publish an open letter to the companies that provide teleconferencing services outlining their privacy concerns relating to this technology.</td>
<td>21 July 2020</td>
<td>Letter</td>
</tr>
<tr>
<td>companies on privacy concerns</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| EDPB opens consultation on Guidelines 07/2020 – the concepts of controller | The EDPB has opened a public consultation on its draft Guidelines 07/2020 on the concepts of controller and processor in the GDPR. The Guidelines are aimed at providing practical guidance on the different concepts of controller and processor in the GDPR, as well as the consequences of each designation. They also emphasise the need for the precise meanings of these concepts and criteria for their accurate interpretation to be sufficiently clear and consistent across the European Economic Area (“EEA”). As well setting out the EDPB’s general observations regarding these concepts, the Guidelines cover the following:  
  - definition of “controller” and “joint controllers”  
  - definition of “processor”  
  - definition of “third party” and “recipient”  
  - consequences of attributing different roles  
  - relationship between a controller and processor; and  
  - consequences of joint controllership  
  The consultation will end on 19 October 2020. | 7 September 2020 | Press release Guidelines |
<p>| and processor in the GDPR                                                   |                                                                                                           |              |                     |
| EDPB releases updated guidelines on the criteria for the right to be        | The EDPB has released its finalised guidance 5/2019 (“Guidelines”) on the criteria of the Right to be Forgotten in the search engine cases under the GDPR, having published these for consultation in 2019. The Guidelines outline the six grounds of | 10 July 2020 | Announcement Guidelines |
| forgotten                                                                  |                                                                                                           |              |                     |</p>
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDPB announces outcome of its 34th plenary session</td>
<td>Following its 34th plenary session, the EDPB has made an announcement summarising the outcome of the session. Firstly, the EDPB announced that it has adopted a statement on the recent Schrems II case. The statement welcomed the CJEU’s ruling. The EDPB has also adopted guidelines on the second Payment Services Directive (&quot;PSD2&quot;) which updates the legal framework for the payment services market. Amongst others, these guidelines reiterate that, in this context, the processing of special categories of personal data is generally prohibited under Article 9(1) GDPR except where explicit consent is given or it is necessary for substantial public interest reasons. The EDPB has adopted a letter in relation to the issues of harmonisation and interoperability of contact tracing applications in the context of the COVID-19 response.</td>
<td>20 July 2020</td>
<td><a href="#">Announcement</a></td>
</tr>
<tr>
<td>EDPB adopts guidelines regarding the targeting of social media users</td>
<td>The EDPB has adopted guidelines on targeting social media users, which provide guidance on the roles and responsibilities of the social media provider and the targeted individual. The guidelines are open for consultation until 19 October 2020.</td>
<td>4 September 2020</td>
<td><a href="#">Press release</a></td>
</tr>
<tr>
<td>EDPS releases report on the use of Data Protection Impact Assessments (&quot;DPIAs&quot;)</td>
<td>The EDPS has issued a report on the use of DPIAs by European institutions, agencies and other bodies (the &quot;Report&quot;). The Report highlights the importance of DPIAs in ensuring the least intrusive means of processing personal data, and states that establishing the rationale and methods of processing personal data is a key functionality of DPIAs to ensure that all those involved in the processing, including the data subjects themselves, understand what is being processed and why.</td>
<td>6 July 2020</td>
<td><a href="#">Press release</a> <a href="#">Report</a></td>
</tr>
<tr>
<td>EDPS publishes checklists for data protection</td>
<td>The EDPS has published a useful infographic covering areas such as the distinction between processors, controllers and joint controllers and respective duties, requirements of a processing agreement, powers of the EDPS and data transfers and Brexit.</td>
<td>6 July 2020</td>
<td><a href="#">Flowcharts and Checklists on Data Protection</a></td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>European Consumer Organisation publishes report on GDPR’s two-year anniversary</td>
<td>The European Consumer Organisation (“BEUC”) has published a report on the effectiveness of GDPR in protecting consumer rights. The report highlights existing problems with the application of the GDPR to the consumer industry, particularly the lack of harmonised procedures to deal with cross-border issues as well as criticising the slow progress of data protection proceedings. In order to address these shortcomings, BEUC has made a number of recommendations, including for example requesting the EDPB to establish a basic framework for a common administrative complaints handling procedure to handle cross-border complaints.</td>
<td>5 August 2020</td>
<td>Report</td>
</tr>
</tbody>
</table>
| ENISA publishes strategy for a “Trusted and Cyber Secure Europe” | The European Agency for Cybersecurity (“ENISA”) has released a new strategy which aims to boost cybersecurity and establish a high level of trust across the EU. The main objectives of the strategy include:  
- creating empowered communities and stimulating active cooperation across the cybersecurity ecosystem;  
- ensuring cybersecurity forms an integral part of EU policies;  
- promoting effective cooperation amongst operational actors within the Union in the event of large-scale cyber incidents;  
- building competencies and capabilities in cybersecurity across the Union;  
- establishing high levels of trust in digital solutions;  
- having foresight on emerging cyber security challenges; and  
- maintaining efficient and effective cybersecurity information and knowledge management. | 17 July 2020 | Press Release Strategy |
| WEF publishes white paper on notice and consent for human technology interaction | The World Economic Forum (“WEF”) has published a white paper (the "Paper") on notice and consent for human technology interaction, which analyses the concepts of notice and consent | 30 July 2020 | Press release Paper |
within the context of data protection and privacy in an ever-evolving digital world.

The Paper highlights perceived problems with notice and consent mechanisms – for example, the length of notices means that consumers rarely read them in any detail before accepting their terms. Furthermore, access to most websites is conditional on consumers agreeing to the privacy and consent statements, meaning that consumers often have no option but to click “I agree”.

Amongst other recommendations, the Paper suggests various alternatives to notice and consent, including data trusts. Data trusts facilitate the fair collection and processing personal data, and would be overseen by a trusted authority who will advocate for the rights of individuals whose data is included in the trust.
Austrian DPA: Statement on international data transfers after Schrems II

Following the Schrems II decision, the Austrian Data Protection Authority ("DPA") published a first short statement on the future of international data transfers. The DPA emphasises that legal data transfers to the US remain possible, if the controller takes the required steps. The DPA lists standard contractual clauses ("SCCs") and Binding Corporate Rules ("BCRs") as possible legal bases for such transfers while clarifying that a controller using SCCs or BCRs will be required to provide additional security guarantees when transferring personal data to the US.

In this regard, the DPA referred to the European Data Protection Board's ("EDPB's") guidelines and FAQs on Schrems II and indicates that it will coordinate the further approach in this matter with the other EU data protection authorities.

Lastly, the DPA stated that there is no grace period in respect of existing Privacy Shield transfers and that Schrems II and its consequences are already legally binding and enforceable.

Austrian NGO 'noyb' files complaints against 101 websites

The Austrian Privacy NGO 'noyb', founded by the Austrian privacy activist Max Schrems, has filed complaints against 101 European websites with different European data protection authorities for alleged GDPR violations. The relevant websites allegedly

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austrian DPA: Statement on international data transfers after Schrems II</td>
<td>Following the Schrems II decision, the Austrian Data Protection Authority (&quot;DPA&quot;) published a first short statement on the future of international data transfers. The DPA emphasises that legal data transfers to the US remain possible, if the controller takes the required steps. The DPA lists standard contractual clauses (&quot;SCCs&quot;) and Binding Corporate Rules (&quot;BCRs&quot;) as possible legal bases for such transfers while clarifying that a controller using SCCs or BCRs will be required to provide additional security guarantees when transferring personal data to the US. In this regard, the DPA referred to the European Data Protection Board's (&quot;EDPB's&quot;) guidelines and FAQs on Schrems II and indicates that it will coordinate the further approach in this matter with the other EU data protection authorities. Lastly, the DPA stated that there is no grace period in respect of existing Privacy Shield transfers and that Schrems II and its consequences are already legally binding and enforceable.</td>
<td>1 August 2020</td>
<td>Statement by the DPA (in German)</td>
</tr>
<tr>
<td>Austrian NGO 'noyb' files complaints against 101 websites</td>
<td>The Austrian Privacy NGO 'noyb', founded by the Austrian privacy activist Max Schrems, has filed complaints against 101 European websites with different European data protection authorities for alleged GDPR violations. The relevant websites allegedly</td>
<td>17 August 2020</td>
<td>Statement by NOYB (in English)</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Date</td>
<td>Links</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>for non-compliance with the Schrems II judgement</td>
<td>continued to use the services Google Analytics and/or Facebook Connect even after the CJEU invalidated the EU-US Privacy Shield in the Schrems II judgement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The NGO claimed that both Google Analytics and Facebook Connect transfer personal data of website users to the US without adequate legal basis for this transfer (following Schrems II). As the owners of the respective websites are controllers of this data transfer, the NGO requested the data protection authorities to prohibit these allegedly unlawful data transfers to the US.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regional Court of Vienna denies most of Max Schrems’ claims in lawsuit against Facebook</td>
<td>The Regional Court of Vienna denied large parts of Max Schrems’ lawsuit against Facebook.</td>
<td>Date of Decision: 17 August 2020</td>
<td><strong>Judgement by the Regional Court of Vienna (in German)</strong></td>
</tr>
<tr>
<td></td>
<td>By way of background, Schrems had filed a lawsuit against Facebook at the Regional Court of Vienna. Amongst other claims, Schrems requested the Court to:</td>
<td>Published: 1 July 2020</td>
<td><strong>Press Release by Max Schrems/noyb (in English)</strong></td>
</tr>
<tr>
<td></td>
<td>− order Facebook to provide him with complete data access under Article 15 GDPR;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>− rule that Schrems himself is controller of the processing of his own personal data in his Facebook profile, while Facebook is only processor of this personal data;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>− require Facebook to conclude a data processor agreement under Article 28 GDPR with him and to order Facebook to cease all processing which he has not instructed;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>− rule that accepting Facebook’s Terms of Service does not constitute valid consent under GDPR; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>− require Facebook to cease processing his personal data for personalised advertisements, in the connection with social plugins in the context of the app “Graph Search” or in the context of personal data collected from third parties without his consent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Court ruled on this case on 30 June 2020. It ordered Facebook to provide Max Schrems with complete data access under Article 15 GDPR and awarded EUR 500 in damages to Max Schrems for this violation.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Development

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>However, Schrems’ other claims were denied, some on formal grounds, others as the Court did not consider Facebook to be in violation of GDPR. The Court ruled that Max Schrems could not be controller of his own personal data on his Facebook profile, as the GDPR’s household exemption would apply to this processing and therefore GDPR could not be applicable to a user’s processing of their own personal data on social media. Furthermore, the Court ruled that personalised advertisements were a significant part of Facebook’s service to its users, so the processing in this regard was justified as it was required for the performance of this contract. Max Schrems has already announced that he will appeal against this judgement to the Regional High Court of Vienna, expecting that the higher Austrian courts will then refer the matter to the CJEU.</td>
</tr>
</tbody>
</table>

### Austrian DPA: Quarterly Report

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>In its quarterly report, the DPA focused on contact tracing apps used in the context of the COVID-19 pandemic. The DPA concludes that the use of such apps is permissible under data protection law, as long as the necessary requirements are met. The DPA is of the opinion that such apps may only be used on a voluntary basis and the users’ consent is required. Furthermore, the personal data may not be used for purposes other than contact tracing (e.g. for supervision of quarantines). Under Article 25 GDPR (data protection by design), the DPA recommends that the collected data should be pseudonymized and contact matching should happen in a decentralized manner.</td>
</tr>
</tbody>
</table>

### Higher Regional Court Linz: Controllers can be liable for GDPR violations by their processors, but only for predictable violations.

<table>
<thead>
<tr>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Higher Regional Court of Linz considered the case of a faulty hair transplantation. The claimant had instructed an Austrian hairdresser (who used a Greek hospital as subcontractor). The treatment was performed in Greece. Without the claimant’s or the Austrian hairdresser’s consent or knowledge, the Greek hospital took photos of the claimant and published them on their website, also naming the claimant and describing his treatment.</td>
</tr>
</tbody>
</table>

---

**Date**

| 29 July 2020 |

**Links**

| Link to Quarterly Report (in German) |

**Date of Decision**

| 17 August 2020 |

**Published**

| 13 August 2020 |

**Link to the decision (in German)**
### The claimant requested EUR 20,000 in immaterial damages from the Austrian hairdresser for the violation of his data protection rights and the humiliation caused by the publishing of his photos.

The Court ruled that the hairdresser could be considered controller of the claimant’s personal data in the context of the treatment and the hospital could therefore be considered processor.

Furthermore, the Court ruled that in principle controllers are liable for damage claims based on data protection violations by their processors.

However, the Court concluded that this only applies to violations that are related to the respective contract and which the controller could have foreseen.

As the Austrian hairdresser could not have foreseen that the hospital would publish the claimant’s data on their website without the claimant’s consent and as this publishing is not intrinsically related to the treatment itself, the court considered that the Austrian hairdresser was not to be liable under GDPR for damage claims for this particular violation by their processor. The claim was therefore denied.

### Austrian DPA: Legal entities have an enforceable right to data protection

An Austrian company distributing pharmaceuticals filed a complaint at the Austrian DPA for alleged violations of the company’s right to data protection.

The DPA clarified that GDPR does not apply to data of legal entities. However, companies and other legal entities nevertheless have a right to data protection guaranteed by the Austrian Federal Constitution. While the scope of this constitutional right is not entirely clear and certainly does not provide the same rights as GDPR, the data of legal entities is protected against undue processing insofar as the processing violates a legitimate interest of the company/legal entity.

Furthermore, legal entities will most likely have the right to request access to data processed about the entity, correction of incorrect data about the company and deletion of data about the entity impermissibly processed.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>The claimant requested EUR 20,000 in immaterial damages from the Austrian hairdresser for the violation of his data protection rights and the humiliation caused by the publishing of his photos.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Court ruled that the hairdresser could be considered controller of the claimant’s personal data in the context of the treatment and the hospital could therefore be considered processor.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Furthermore, the Court ruled that in principle controllers are liable for damage claims based on data protection violations by their processors.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>However, the Court concluded that this only applies to violations that are related to the respective contract and which the controller could have foreseen.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>As the Austrian hairdresser could not have foreseen that the hospital would publish the claimant’s data on their website without the claimant’s consent and as this publishing is not intrinsically related to the treatment itself, the court considered that the Austrian hairdresser was not to be liable under GDPR for damage claims for this particular violation by their processor. The claim was therefore denied.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>An Austrian company distributing pharmaceuticals filed a complaint at the Austrian DPA for alleged violations of the company’s right to data protection.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The DPA clarified that GDPR does not apply to data of legal entities. However, companies and other legal entities nevertheless have a right to data protection guaranteed by the Austrian Federal Constitution. While the scope of this constitutional right is not entirely clear and certainly does not provide the same rights as GDPR, the data of legal entities is protected against undue processing insofar as the processing violates a legitimate interest of the company/legal entity.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Furthermore, legal entities will most likely have the right to request access to data processed about the entity, correction of incorrect data about the company and deletion of data about the entity impermissibly processed.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Date of Decision:** 17 August 2020

**Published:** 24 August 2020

[Link to the decision (in German)](#)
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>While this is not explicitly stated in the Austrian Data Protection Act, the DPA has stated that violations of a legal entity’s right to data protection can be enforced by complaints to the DPA.</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Austrian Federal Administrative Court: No right to partial deletion of personal data in a credit database.</strong></td>
<td>The controller, a credit agency, had processed the complainant’s personal data in the context of a credit score data base. The complainant requested deletion of certain data detrimental to his credit status, which he considered incorrect and outdated, from this database, while requesting that the general data about him remain within the database. Following the request, the controller deleted all personal data about the complainant from the credit score data base. However, the complainant filed a complaint against this, requesting that the general information about him be reinstated into the database, as he claimed that due to no data about him being available in the credit score database, he was unable to apply for new insurance at his insurance provider. The Austrian DPA denied the claim. The Austrian Federal Administrative Court confirmed this decision by deciding that there was no right to a partial deletion of records. GDPR also does not grant the right to request a controller to reinstate deleted data, regardless of the reason for deletion.</td>
<td>Date of decision: 17 August 2020</td>
<td>Link to the decision (in German)</td>
</tr>
<tr>
<td><strong>Austrian Federal Administrative Court: Credit agencies must disclose the logic behind the calculation of credit score</strong></td>
<td>A data subject filed a data subject access request to a credit agency pursuant to Article 15 GDPR. Amongst other things, the credit agency informed him about the factors that were used to calculate his credit score. However, it refused to give further information on how exactly the credit score was calculated from these factors, as it claimed that this would mean disclosure of trade secrets. Following an appeal against the decision by the Austrian DPA in this matter, the Austrian Federal Administrative Court ruled that under Article 15 (1h) GDPR, the data subject has a right to also receive information on the exact calculation of the credit score. The mere claim that this information is subject to the agency’s trade secrets was not sufficient to deny the request. However, if (and only if) the credit agency can comprehensively explain and prove to the data subject that certain parts of the calculation process are in fact trade secrets, it is permissible to exclude these</td>
<td>Date of Decision: 17 August 2020</td>
<td>Link to the Decision (in German)</td>
</tr>
</tbody>
</table>
### Development Summary

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>parts (and only these parts) from the response to the data subject access request.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The credit agency has appealed against this decision to the Austrian Supreme Administrative Court. However, the decision has been declared preliminarily enforceable.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Draft Data Security Law

On 3 July 2020, the Standing Committee of the National People’s Congress of China published the Draft Data Security Law (“Draft DSL”) for public comments. The Draft DSL aims to, amongst other things, protect data security and promote the use of data. It applies to any entities conducting data activities within the PRC. The key provisions are summarised below:

- It applies to both PRC and overseas entities (i.e. it has extra-territorial effect). Irrespective of whether the organisation is a PRC-incorporated entity or foreign company collecting data within the territory of China, the Draft DSL will apply to such data activities which may harm the PRC’s national security, public interests, or the legal rights of PRC citizens and organisations.

- If an organisation processes "important data", it is required to appoint a data security officer. Furthermore, organisations also need to establish a data management body, regularly carry out risk assessments in relation to their data processing activities and submit assessment reports to the relevant supervisory authorities.

- If an organisation operates an online data processing service business, it is required to obtain a relevant business licence.

Draft Data Security Law
Details of such licence will be announced by the Ministry of Industry and Information Technology.

- organisations need to obtain official approval before providing overseas regulatory authorities with requested data from or stored in the PRC. Upon receiving a request from an overseas regulatory authority for such data, the organisation is required to report this request to the relevant supervisory authority in the PRC.

- the relevant authority may request an “in-person consultation” for the purpose of exercising its supervisory obligations. Organisations should also take remedial measures to eliminate data security vulnerabilities as requested by the relevant authority.

- catalogues on the protection of important data will be created by local authorities. Such catalogues will provide further guidance on the scope of “important data”. Currently, there is no clear scope of important data.

- a data grading and classification system will be established. Such system will grade and classify data according to the impact on national security, the public interest, and the lawful rights and interests of Chinese citizens or organisations if the data is falsified, destroyed, leaked, illegally retrieved or illegally used.

Under the Draft DSL, non-compliance will be subject to a range of sanctions, including (but not limited to) correction orders, warnings, revocation of business operation licences, confiscation of profits arising from illegal data activities, a fine of up to RMB 1,000,000 (if no profits are made from illegal data activities), or a fine equal to ten times the profits arising from illegal data activities (if any). Furthermore, implicated individuals may also be subject to a fine of RMB 100,000. In addition, other administrative or even criminal liabilities may be pursued under severe circumstances.

### Practice Guide on Network Security Standard – Self-assessment Guide for the Collection and Use of Personal Data in Mobile Internet

Internet Applications (Apps) (the “Guide”) to provide guidance to operators of apps, mini apps/programmes and quick apps on the collection and use of personal data in apps. Specifically, the Guide provides comprehensive assessment criteria for operators to self-assess whether they have complied with the requirements in the PRC Cybersecurity Law and other laws or regulations relevant to the collection and use of personal data. These self-assessment criteria are summarised below:

- disclosure of data collection policies. The rules and policies for the collection and use of personal data, including the policy on privacy, shall be disclosed in a manner which is easy to discover, access and read, and shall contain full disclosure on the operator's information, the purpose, method and scope of data collection and storage location for the collected personal data etc.

- disclosure of purpose, method and scope. The purpose, method and scope of the collection and use of personal data shall be explicitly disclosed and if changed, notified to the data subject.

- consent from data subject. Consent should be obtained from the data subject before the collection and use of personal data. If data subject refuses to provide such consent, personal data should not be collected and data subject should not be harassed. The personal data collected shall not exceed the scope to which data subject has consented and authorised. Furthermore, an appropriate channel shall be provided for the data subject to withdraw their consent.

- principle of necessity. Operators should abide by the principle of necessity and only collect personal data necessary for and related to the service being provided. Data subjects should be free to reject requests for unnecessary personal data and authorization and shall not be forced to provide them.

- consent before passing on data to third party. Consent should be obtained from data subject before his/her personal data is passed on to a third party or a third party app.
Proper channels should be provided to data subjects to remove/update personal data and the procedures to file complaints or reports should be made clear. In case the app requires users to register an account, there should be functions to deregister the account.

On 22 July 2020, the Ministry of Industry and Information Technology announced the launch of its operation to rectify infringement of user rights and interests by apps (the “Notice”). The purpose of the operation was to deepen the integration of technology and management, strengthen supervision and inspection, prompting relevant companies to strengthen personal data protection in apps, and ensuring timely rectification and elimination of outstanding issues.

The operation targets parties including app providers, software development kit providers and application distribution platforms. It focuses on rectifying issues related to (i) illegal collection and use of user personal data (ii) harassment of users (iii) deceiving and misleading users, and (iv) insufficient implementation of application distribution platform management responsibilities.

The operation will achieve the above through (i) inspection and review; (ii) enforcement actions; (iii) promotion of self-discipline in the industry; (iv) strengthening of the review system; and (v) ensuring a clear channel for complaints.

On 31 August 2020, the State Administration for Market Regulation and the State Standardization Administration jointly published the Information security Technology - Cyber-data process security specification (Exposure Draft) (the “Draft Specification”) for public comments. The Draft Specification concerns the collection, storage, use, process, transmission, provision and publication of data through the network by network operators, and provides for standards and security requirements in this regard.

The Draft Specification requires network operators to identify data involved in the data processing activities, formulate an index of data accordingly and update in time. Data shall be classified and accorded with different protective measures. Network operators should be able to conduct security impact assessments and conduct security reviews.

Notice by the Ministry of Industry and Information Technology on launching a special operation to rectify infringement of user rights and interests by apps

Information security technology - Cyber-data process security specification (Draft for Consultation)
operators carrying out data processing activities are required to take necessary measures to strengthen data security protection, and protect data from leakage, theft, tampering, damage, and improper use. They shall also establish a data security management responsibility and evaluation system, formulate a data security protection plan, carry out security risk assessments, deal with security in a timely manner, and organise education and training. Furthermore, network operators are required to record the entire life cycle of data processing activities to ensure that data processing activities are auditable and traceable.

In addition, the Draft Specification requires network operators which collects important data and sensitive personal data to appoint a responsible person for data security and provide necessary resources to guarantee that he/she can independently carry out his/her duties, which are inclusive of formulation of data protection index, data protection plan, carry out risk assessments and analysis, report to the competent authorities on data protection incidents and handle any complaints in this regard.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
</table>
| Regulation on Management of Commercial Cryptography (Draft Amendments for Consultation) | On 20 August 2020, the State Cryptography Administration published the Regulation on Management of Commercial Cryptography (Exposure Draft) (the “Draft Regulation”) suggesting comprehensive amendments to the "Regulations on the Administration of Commercial Cryptography" (published in 1999). The Cryptography Law of the PRC (the “Cryptography Law”) (which took effect on 1 January 2020) introduced structural changes to the management system of commercial code. The Draft Regulation was therefore published to make corresponding amendments which deal with the new changes introduced by the Cryptography Law, including:  
  - redefining the scope of the regulation. The scope of regulation was widened beyond cryptographic technology and products to include commercial cryptographic services  
  - testing and certification for commercial cryptography – the management of commercial cryptography in the PRC has moved from an “approval based” system to a “test and certification” system. The Draft Regulation follows the test and certification system adopted by the Cryptography Law, and further specifies the qualification required of the test and | 20 August 2020 | Regulation on Management of Commercial Cryptography |
crediting institutes, application procedure, competent authorities, inspection and management of the process

- electronic certification – the Draft Regulation specified the qualification required of electronic certification service providers, whose service may be used in conjunction with electronic signatures, and in particular, electronic certification service providers for electronic government work

- import and export of commercial cryptography – The Cryptography Law changed the control on the import or export of the commercial cryptographic technology and products from a system based on government approval to one that is based on “permitted list” for import and “restricted list” for export. The Draft Regulation further substantiated the import and export control imposed, including the requirement to apply for an Import and Export Permit

- synergy with Multi-Level Protection Standards ("MLPS") – the Draft Regulation adopts the cybersecurity standard specified under the MLPS 2.0. Further, since the cybersecurity standards specified under MLPS 2.0 are merely recommended standards, the Draft Regulation, if passed, shall elevate such standards to an enforceable status

- national security review – the Draft Regulation subjects the purchase of commercial cryptographic products and services by operators of critical information infrastructure to national security review; and

- encouraging use of commercial cryptography – the Draft Regulation encourages the use of commercial cryptography by implementing measures, including but not limited to, protect intellectual property in commercial cryptography and specifying for the establishment of a comprehensive innovation and promotion mechanism for commercial cryptography
The CNIL publishes three reference documents for the healthcare sector

Three new reference documents have been adopted by the French Data Protection Authority ("CNIL") which are intended to help controllers to manage day-to-day processing in medical and paramedical practices, and assist them in determining retention periods.

The first reference document relates to the management of day-to-day processing in medical and paramedical practices. This document is not binding, so controllers may depart from its recommendations (for example, by identifying other legal bases for a specific processing, etc.), provided they can justify their choices (and remain responsible for such departure).

The other two reference documents relate respectively to the recommended data retention periods for (i) data processing implemented for the purposes of research, study and evaluation in the health sector, and (ii) data processing in the health sector outside of research (e.g. maintenance of patient records, etc.).
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>prescriptions, health vigilance, etc.). The standards set out in these documents aim to facilitate decision making by controllers by directing them to:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>− the mandatory retention periods resulting from the relevant regulations in force, in particular the French Public Health Code; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>− the retention periods recommended by the CNIL, which are benchmarks for determining the relevant retention period.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Codes of conduct: publication of the accreditation standard for inspection bodies**

Article 40 of the GDPR provides that associations and other bodies representing categories of controllers or processors may prepare codes of conduct, which are sector-specific compliance tools. They allow the representatives of a sector of activity to accompany the compliance of the professionals concerned via practical and operational recommendations.

When preparing a code of conduct, the relevant association or body representing the sector must organise the monitoring of the code after its approval. To this end, Article 41 of the GDPR provides for the intervention of a third party organisation that must be approved by the CNIL in order to fulfil this task.

The CNIL has just published the accreditation standard (which has received a favourable opinion from the European Data Protection Board), making it possible to verify that the future control body provides all the necessary guarantees to fulfil its duties as detailed above.

The relevant requirements under the accreditation standard include:

− the independence of the control body, as well as the absence of any conflict of interest;
− the appropriate level of expertise of the control body;
− specific security measures;
− transparent handling of complaints;
− regular control procedures; and

<p>| 24 July 2020 | CNIL statement (in French) | FAQ (in French) |</p>
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
</table>
| **The CNIL publishes a practical guide and handbook concerning authorised third parties** | Some authorities have the power to require organisations to transmit documents or information that may include personal data – such authorities are considered “authorised third parties”. In order to assist organisations upon receiving this type of request from an authorised third party, the CNIL has published a practical guide and handbook which sets out the most common procedures. The guide describes the issues that controllers may encounter, and the points to be checked before responding to a request from an authorised third party. These include, in particular:  
- obtaining a written request for communication specifying the legal basis of the request;  
- verifying that the scope of the request complies with the legal provisions invoked;  
- ensuring the application of confidentiality measures in order to secure the transfer; and  
- preservation of the traceability of the transfers and verifications carried out.  
The handbook describes nearly one hundred of the most common procedures that may be implemented by authorised third parties.                                                                                      | 10 July 2020   | CNIL statement (in French)  
Practical guide (in French)  
Handbook (in French)                                                                 |
| **The CNIL serves formal notice to several employers in connection with the use of badge systems that photograph employees** | In 2018, the CNIL received six complaints from employees denouncing the installation of badge-based access control systems by their employer including systematic photography at each check-in.  
The CNIL carried out four inspections between March and September 2019 to confirm the use of these systems. As a result, the CNIL decided that the use of these systems was infringing the principle of data minimisation.                                                                 | 27 August 2020 | CNIL statement (in French)                                                                 |
As a reminder, any system for controlling working hours must comply with the principle of data minimisation set out in section 5(1.c) of the GDPR. Thus, the data collected must be adequate, relevant and limited to what is necessary for purposes for which they are processed. This principle is also echoed in article L.1121-1 of the French Labour Code which provides that: "nobody may place restrictions on the rights of individuals and on individual and collective freedoms that are not justified by the nature of the task to be performed or proportionate to the purpose pursued".

The Conseil d'État (French administrative supreme court) and the Cour de cassation (French judicial supreme court) have already had occasion to specify, with regard to a system ensuring the control of employees' working hours by collecting their geolocation data, that "the use by an employer of a geolocation system to ensure the control of the working hours of its employees [...] is lawful only when this control cannot be carried out by any other means, even if it is less effective".

In the cases at issue, the CNIL considered that the mandatory and systematic collection (two to four times a day) of employees’ photographs at clocking in/off points was excessive.

The CNIL pronounced its first sanction decision as lead supervisory authority

The CNIL pronounced a sanction of EUR 250,000 against a company which specialises in the online sale of shoes, with a website accessible in 13 Member States of the EU.

The CNIL audited the company in May 2018, and found breaches in respect of customer, prospect and employee personal data. The CNIL therefore decided to initiate sanction proceedings against the company in 2019.

As the data subjects concerned were located in several European countries, the CNIL cooperated throughout the procedure with the other European supervisory authorities concerned in order to adopt the decision to impose sanctions.

Following the investigation, the CNIL considered that the company had failed to comply with several obligations under the GDPR:

- failure to comply with the principle of data minimisation. The full and permanent recording of telephone calls received by
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer service employees was excessive – the person responsible for employee training was only listening to one recording per week and per employee. The recording and retention of customers' bank details communicated for orders placed by telephone was also unnecessary for the purpose of employee training. In the context of fraud prevention, the collection in Italy of copies of customers' &quot;health cards&quot; was excessive and irrelevant.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>− failure to comply with the principle of storage limitation. At the time of the CNIL's inspection, no retention period for customer and prospect personal data was set up by the company, which did not regularly erase or archive personal data. The CNIL identified a breach of the GDPR in relation to the company's retention for several years of a very large number of data from former customers (more than 3 million customers had not logged on to their account for more than 5 years). Concerning the data of prospects, the company has implemented a retention period of five years from their last activity (for example the opening of a newsletter). However, the company did not send direct marketing communications to these people if they did not show interest in its products or services for two years. The CNIL therefore considered that the retention of prospect data was not necessary beyond this two-year period. The CNIL also specified that the mere opening of a direct marketing e-mail by an individual does not demonstrate that he or she is interested in the company's products or services - which justifies the retention of his/her data - insofar as this message may be opened involuntarily by the company. After the five-year retention period for customer data, customers' e-mail addresses and passwords were retained in a non-anonymised form to allow them to log back into their account. This was also found to be in breach of the GDPR.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| − a failure to comply with the principle of transparency. The information provided in the privacy policy of the website was not compliant since the company indicated that consent was the legal basis for all processing carried out, when in fact much of their data processing was based on other legal bases such as contract or legitimate interests pursued by the
company. With regard to employees, the information relating to the recording of telephone calls made with customers was also insufficient. Employees were not informed of the purpose and legal basis of the processing, the recipients of the data, how long the data would be kept and their rights

- a failure to ensure an appropriate level of security of the data. With respect to passwords for accessing customer accounts via the website, the company should have required users to use stronger passwords. In the context of fraud prevention, retention for six months and (in clear text) of the scans of the credit card used for an order did not guarantee the security of customers' banking data

Taking into account the number of breaches, the CNIL imposed a fine of EUR 250,000 and decided to make its sanction public. It took into account the seriousness of the breaches, particularly in relation to the recording of telephone conversations and the retention of bank data. It also took into account the number of data subjects concerned, with the data of several thousand people being retained beyond the necessary periods (more than 3 million former customers and more than 25 million prospects). The CNIL also stated that several of the breaches were essentially related to obligations that already existed prior to the GDPR.

"Listening to you": the CNIL publishes its white paper on voice assistants

Because of their presence in smartphones, cars and even refrigerators, voice assistants have become indispensable. In order to explore the ethical, technical and legal issues involved, the CNIL has published a white paper for professionals and users.

The whitepaper presents best practices for designers, app developers, and other organisations wishing to use voice assistants technologies, emphasising the need for transparency and security of the devices designed in order to respect the GDPR and the privacy of individuals.

Guidance is also provided to users on how to control their voice assistants, for example to ensure the confidentiality of the data transmitted, the use made by children, and the security of the devices.

In addition to the publication of this white paper, the CNIL has updated the content dedicated to voice assistants on its website.
## Development

| The CNIL publishes a charter to clarify its inspection procedure | The CNIL has several missions and powers, including the ability to control and sanction organisations that do not comply with the GDPR or the French Data Protection Act (Loi Informatique et Libertés no.78-17). These controls also make it possible to assess new issues in terms of data protection and privacy. Inspections may be carried out at a company’s premises by invitation, online or on the basis of documents, although such inspections are closely regulated. In 2019, 300 inspections were carried out, including 53 online and 45 documentary inspections. While complaints and claims are a major source of controls (43% in 2019), the CNIL can also carry out investigations on its own initiative, for example in response to current events. In addition, each year it draws up a program of priority topics for future inspections. Because of the particularly high stakes involved in these inspections, it is essential that the organisations concerned understand how these investigations are carried out and how the CNIL can intervene. The purpose of the CNIL's charter is therefore to emphasise, as precisely as possible, the rights and obligations of the organisations subject to inspections, particularly with regard to the French Data Protection Act and the GDPR. The CNIL also specifies the conduct and consequences of an inspection, whatever its form, as well as the principles of good practice to be followed in this context. | 1 September 2020 | CNIL statement (in French)  
CNIL charter (in French) |
| The Ombudsman for companies and the CNIL join forces to resolve disputes in contractual relationships | Since the entry into force of the GDPR, both the CNIL and the Ombudsman for companies (Médiateur des entreprises) have seen an increase in the number of contractual disputes related to a misunderstanding or misapplication of the respective obligations of controllers and their processors. This is the case across all business sectors, administrations or companies, whether small companies or multinational groups. In addition, the health crisis has caused a double phenomenon: | 16 September 2020 | CNIL statement (in French) |
on the one hand, an acceleration in the digital transformation of businesses, particularly through the development of home working and online sales; and

− on the other hand, a profound economic crisis hitting a large majority of small companies

These tensions will undoubtedly have repercussions on the contractual relationships controllers/processors, and are likely to increase the number of disputes, including on the sharing of responsibilities with respect to the GDPR.

In order to help both companies and public bodies (local authorities, public institutions etc) to comply with their contractual relationships by having a good understanding of their respective obligations, the CNIL and the Ombudsman for companies have signed a partnership agreement to provide support - offering free, confidential and neutral assistance to companies who face contractual or relational difficulties with a customer or supplier.
The Commissioner for Data Protection and Freedom of Information of Berlin urged all organisations in Berlin who save personal data in the US to move this data and save it in Europe, following the Schrems II decision. The Commissioner embraced the Schrems II decision of the Court as it clearly states that data transfers are not a purely economic issue, rather the rights of the individual have to be prioritised, and that the time where data was transferred to the US for cost and convenience is over. The

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Commissioner for Data Protection and Freedom of Information of Berlin on the Schrems II decision</td>
<td>The Commissioner for Data Protection and Freedom of Information of Berlin urged all organisations in Berlin who save personal data in the US to move this data and save it in Europe, following the Schrems II decision. The Commissioner embraced the Schrems II decision of the Court as it clearly states that data transfers are not a purely economic issue, rather the rights of the individual have to be prioritised, and that the time where data was transferred to the US for cost and convenience is over. The</td>
<td>17 July 2020</td>
<td>Press Statement (in German)</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>---------</td>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>Commissioner also pointed out that transfers to other countries such as India, Russia or China will also have to be inspected to whether the same of greater issues are present with regard to the data protection standard in respect of protection for transferred personal data under Standard Contractual Clauses (“SCCs”).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>The Commissioner for Data Protection and Freedom of Information of Baden-Württemberg released a set of guidelines in response to the Schrems II judgment</strong></td>
<td>After the <em>Schrems II</em> decision invalidated the Privacy Shield for data transfers to the US and made clear that SCCs only remain applicable under further conditions, the Commissioner for Data Protection and Freedom of Information of Baden-Württemberg released a set of guidelines in regards to the international transfer of data, with a focus on who is affected by the judgement and what measures are recommended for companies to remain compliant with the judgement and the GDPR.</td>
<td>25 August 2020</td>
<td>Guidelines (in German)</td>
</tr>
<tr>
<td><strong>The Commissioner for Data Protection and Freedom of Information of the Rhineland Palatinate on the consequences of the Schrems II decision</strong></td>
<td>Following the <em>Schrems II</em> decision, the Commissioner stated that Privacy Shield cannot be used as a basis for data transfers to the US, and that he will contact companies to check whether they have been transferring data on the basis of Privacy Shield. SCCs can be used if extra steps are taken to ensure that the European data protection standard is kept. In the Commissioner’s opinion, for the US this will rarely be the case, even though on a case-by-case basis, the standard might be reached. Meanwhile data transfers to other countries have to be revised to control whether the standards align with the one required, which has always been the case, but now is even more imperative. The Commissioner further points out that data transfers have to cease if the standards set out by the GDPR and the <em>Schrems II</em> decision by the Court. If personal data has been transferred on the basis of Privacy Shield, this data has to be reclaimed or destroyed, with this being documented. Failure to do so can be sanctioned.</td>
<td>24 July 2020</td>
<td>Press statement (in German)</td>
</tr>
<tr>
<td><strong>The Commissioner for Data Protection and Freedom of Information of Berlin publishes the results of the testing of video conference providers</strong></td>
<td>The Commissioner for Data Protection and Freedom of Information of Berlin published the results of testing the services video conference providers, which was initiated due to the flood of enquiries about video conferencing during the COVID-19 pandemic. The relevant video conference services were reviewed initially from the perspective of the data processing agreements that the data controller is required to enter into with the relevant service provider, and some technical aspects of the services. If</td>
<td>3 July 2020</td>
<td>Press statement (in German)</td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Date</td>
<td>Links</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>the Commissioner identified problems during this initial process, it stated that the service should only be used if additional agreements between the parties are put in place. To make it easier to distinguish between the relevant services and related issues, a traffic light system was used, with green (no faults), amber (faults which can be remedied without significant changes), and red (faults which cannot be easily remedied). The list will continue to be updated by the Commissioner, with relevant video conference service providers being encouraged to provide contractual and technical documents for assessment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Data Protection Conference published guidance on the conditions under which the use of thermal imaging cameras or electronic temperature recording is permitted in the context of the COVID-19 pandemic. The guidance makes clear that processing personal data obtained by temperature, which as health data is subject to special protection, is only permitted in accordance with Article 9 GDPR (and in addition in accordance with Article 6 GDPR). In this respect, consent cannot generally be assumed (where not voluntary and also due to a general lack of transparency). In respect of the lawful bases for processing set out in Article 6 GDPR: ‘contract performance’ is not applicable (since, in the case of access control, the temperature measurement is not carried out for the fulfilment of an existing contractual relationship between the parties); neither is there a specific legal obligation to take electronic fever measurements; and neither will consent be available where the individual is unable to give consent (as such consent is not valid). However, for companies and other non-public bodies, ‘legitimate interest’ under Article 6 GDPR may be available, which - to put it briefly - allows processing on the basis of a balancing of interests if it is necessary to safeguard legitimate interests and if the interests of the data subject do not prevail.</td>
<td>10 September 2020</td>
<td>Resolution of the Data Protection Conference (in German)</td>
</tr>
<tr>
<td></td>
<td>By way of background, during the course of COVID-19, restaurants in Bavaria are obliged to collect contact data of their guests in order to better trace chains of infection. From a data protection perspective, the principle of confidentiality and integrity must be observed, which amongst others means the personal data collected must be stored in such a way that third</td>
<td>25 June 2020</td>
<td>Press statement (in German) Sample data entry form (in German)</td>
</tr>
</tbody>
</table>
contain COVID-19 and the misuse of the Corona Warning App

A sample data entry form has been made available for use in the gastronomy sector for these purposes, by the Bavarian Data Protection Authority for the Private Sector.

In addition, the Authority dealt with the question of whether restaurants or employers may check or prescribe the use of the Corona Warning App by their guests or employees. The Authority stated that there is in particular no viable lawful basis for employers who want to oblige their employees to use the App or to check the status of the App, or for companies who want to check the use of the App to process data for operational purposes. The consent given by the App user when installing the App does not include the purposes of access control and/or operational infection prevention pursued by the employer/company, and even a separate consent for these purposes could not be used as a lawful basis for the processing, as such consent would not have been voluntarily given.

The Commissioner for Data Protection and Freedom of Information of Baden-Württemberg on the problems of facial recognition

The Commissioner for Data Protection and Freedom of Information of Baden-Württemberg has stated that it is alarmed by the development of facial recognition software. In its press statement on this issue, the Commissioner commented on a Polish platform, which is able to use facial images on its database to search for the same face across the internet and which can be used by third parties. The Commissioner stated that the taking and uploading of pictures to a facial recognition software platform constitutes a breach of a person’s right to their own image.

Furthermore, the subsequent processing of the image on the platform, will not have a lawful basis, and therefore such processing cannot take place without the consent of the party concerned (in order to provide a lawful basis). As per the Commissioner, this service provided by the platform has the impact of infringing the rights of other individuals in respect of their own image, if a user uploads another individual’s image. Furthermore, the Commissioner highlighted the dangers of a development such a this in regards to a person’s anonymity in a democratic society (especially in regards to demonstrations) and warned that this large-scale collection of images could be the first
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Federal Commissioner for Data Protection and Freedom of Information on the consequences of the Patient Data Protection Act’s (PDSG) infringement of GDPR</td>
<td>The Federal Commissioner for Data Protection and Freedom of Information stated that the processing of personal data relating to health (electronic patient record) in accordance with the Patient Data Protection Act (PDSG) will infringe GDPR, and that as a result it will have to take action against the statutory health insurance companies if the PDSG is implemented in its current version.</td>
<td>19 August 2020</td>
<td>Press statement (in German)</td>
</tr>
<tr>
<td>The Commissioner for Data Protection and Freedom of Information of Baden-Württemberg announces review of tracking technology on websites</td>
<td>Together with other German supervisory authorities, the Commissioner for Data Protection and Freedom of Information of Baden-Württemberg announced that it will comprehensively check the use of tracking technologies in relation to online sales in accordance with legal requirements. The websites of media companies which generally make frequent use of such tracking technology will be checked first, and may only use the tracking technologies if the user effectively consents to their use (i.e. is fully informed and in advance voluntarily consents, separately and in the knowledge of a reasonable possibility to revoke the consent at any time).</td>
<td>19 August 2020</td>
<td>Press statement (in German)</td>
</tr>
<tr>
<td>Regional Labour Court Düsseldorf decided that a works council cannot inspect the electronic personnel file of employees without employee approval</td>
<td>The general right of works council chairmen to inspect the electronic personnel file of employees, without their consent, violates the general personal rights of employees under the German Constitution, which the works council parties must observe under the Works Constitution Act. In this case, a general works council was set up in a company, which stipulated in its general works agreement that the works council should have access to almost all personnel files. The Court decided that such a far-reaching right of inspection by the works council was neither appropriate nor necessary and violated the general personal rights of employees.</td>
<td>1 July 2020</td>
<td>Press statement of Court (in German)</td>
</tr>
<tr>
<td>Higher Administrative Court of Niedersachsen decides that fax transmission of personal data infringes GDPR</td>
<td>The transfer of personal data by fax (in this case amongst others: name; address; and vehicle registration number by a public authority) infringes GDPR where the personal data concerned is particularly sensitive and requires special protection.</td>
<td>22 July 2020</td>
<td>Judgement (in German)</td>
</tr>
</tbody>
</table>
### Development Summary

The Court found that the transmission of information by fax without encryption is comparable to sending an open postcard. Sensitive personal data should not be faxed without back-ups (e.g. encryption devices) because there is a risk that unauthorised third parties could access the personal data.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Supreme Court (BGH) approves Federal Cartel Office order against Facebook</td>
<td>In summary proceedings, the Federal Supreme Court (BGH) ruled on June 23, 2020 on a prohibition order issued by the Federal Cartel Office against Facebook. In February 2019, the Federal Cartel Office found an infringement of competition in the form of an abuse of market power on the part of Facebook in relation to its terms of use and as a result demanded these were changed. The issue in relation to Facebook’s terms of use was as follows. All users must agree to these before they can use the social network. This agreement to the terms of use then allows Facebook to evaluate data from the use of its own services, such as Instagram and WhatsApp, as well as data from third-party websites, such as Facebook Pixel or the Like Button. In the Court’s opinion, such usage of the terms of use constitutes abuse of a dominant market position, and simultaneously, Facebook thus violates GDPR, as it makes the private use of the network dependent on the user's consent to collect, combine and evaluate the user data. Since Facebook has a virtually unique selling point among social networks due to its size, the user's consent is not voluntarily given due to lack of an alternative.</td>
<td>1 July 2020</td>
<td>Press statement of court (in German)</td>
</tr>
</tbody>
</table>
The Privacy Commissioner for Personal Data ("PCPD") responded to personal data privacy issues in relation to the Universal Community Testing Programme for COVID-19 (the “Programme”).

In response to the Government’s earlier enquiries over public’s concern on the potential privacy issues arising from the Programme, the PCPD had provided its views in support of the Government not breaching the requirements of the PDPO in terms of the collection, holding, processing or use of personal data. In particular, the PCPD found that:

- as regards data collection process, the Government had collected necessary but not excessive personal data, which is in line with the principle of personal data minimisation and is

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Privacy Commissioner for Personal Data (&quot;PCPD&quot;) responded to personal data privacy issues in relation to the Universal Community Testing Programme for COVID-19 (the “Programme”)</td>
<td>In response to the Government’s earlier enquiries over public’s concern on the potential privacy issues arising from the Programme, the PCPD had provided its views in support of the Government not breaching the requirements of the PDPO in terms of the collection, holding, processing or use of personal data. In particular, the PCPD found that:</td>
<td>28 August 2020</td>
<td>Media statement</td>
</tr>
</tbody>
</table>
In issuing the Statement, the SFC has committed to complying with the requirements under PDPO as regards preserving personal data privacy. As a breakdown, the SFC has categorised a variety of personal data collected via different forms/sections of the SFC’s website or the general visiting of it, and the respective purposes of use and limitations and duration of retention of such person data by their means of provision from the relevant data subject.

Notable exceptions to the above general commitment being that, if for purposes including, among other things, prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, and protecting the public from financial loss arising from certain acts, the information of a complainant so provided to SFC can be used inconsistently with the data protection principles under the PDPO, whether or not the relevant complainant gives consent.

The SFC specifically sets out that certain personal data relating to licensed registered persons may be contained in the public registers it maintains and subsequently be published in pursuance of law.

The Securities and Futures Commission (the “SFC”) issued a privacy policy statement (the “Statement”) committing to compliance with the Personal Data (Privacy) Ordinance (the “PDPO”).

In issuing the Statement, the SFC has committed to complying with the requirements under PDPO as regards preserving personal data privacy. As a breakdown, the SFC has categorised a variety of personal data collected via different forms/sections of the SFC’s website or the general visiting of it, and the respective purposes of use and limitations and duration of retention of such person data by their means of provision from the relevant data subject.

Notable exceptions to the above general commitment being that, if for purposes including, among other things, prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, and protecting the public from financial loss arising from certain acts, the information of a complainant so provided to SFC can be used inconsistently with the data protection principles under the PDPO, whether or not the relevant complainant gives consent.

The SFC specifically sets out that certain personal data relating to licensed registered persons may be contained in the public registers it maintains and subsequently be published in pursuance of law.

The Statement
Furthermore, the Statement also provides means for the public to request access to and correction of their personal data held by the SFC by way of writing to a designated address of the SFC.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
</table>
| The PCPD responded to media enquiry on cyberbullying                       | Cyberbullying generally refers to bullying behaviour online which mostly takes place among friends for the purpose of venting resentment, primarily involving misuse of personal data and hence a contravention of the requirements of Data Protection Principle 3 of the PDPO. It is distinguished from a criminal doxxing which refers to disclosure of personal data obtained without consent of the data user concerned who holds the data, coupled with intimidating or incitement messages which may cause psychological harm to the data subjects concerned. The PCPD was invited via media enquiry to give its response to the below three questions:  
  - how many reports of cyberbullying did you receive from January to June this year?  
  - How many reports of cyberbullying did you receive last year?  
  - What can a bullied person do; what can PCPD do upon receipt of a compliant? What are the governing laws and regulations?  
  During the year ended 31 December 2019, PCPD received 69 complaints on cyberbullying whereas, during the half year ended 30 June 2020, it received 157 complaints on cyberbullying.  
  In its response, the PCPD stressed that victim with some evidence of cyberbullying can complain to it and such complaint will be handled with strict confident per the PDPO. Under PDPO, even cyberbullying based on the use of personal data of targeted persons collected from public sources could be found a breach of PDPO which shall attract, in the absence of the wrongdoer complying with the enforcement notice, a maximum fine of HK$50,000 and maximum imprisonment for two years and, in the case of a continuing offence, a daily fine of HK$1,000. | 8 July 2020 | Media Statement         |
<p>| The PCPD responded to disclosure of personal data of Hong Kong SAR         | In relation to the press release made by the US Department of the Treasury dated 7 August 2020, content of which contained the Disclosure, the PCPD noted that, despite that the Federal | 8 August 2020 | Media Statement         |</p>
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>officials and others by the US Government (the “Disclosure”)</td>
<td>Register, the government body of the United States that published the Executive Order, based on which the press release was made public (akin to the Gazette of Hong Kong), the Disclosure is obviously excessive and amounts to doxxing. The PCPD acknowledged the lack of extra-territorial powers of the PDPO over control of the collection or use of personal data outside Hong Kong, but have contended that data protection authorities in many jurisdictions have been advocating practising data ethics to ensure respectful, fair and beneficial handing of personal data, and that the Disclosure diametrically contravenes such data ethics. The PCPD will write to its counterpart in the US to make its disappointment known. As regards the use of the underlying personal data in Hong Kong, the PCPD appealed to the community not to improperly use or reproduce the personal data contained in the Disclosure as it might lead to a criminal offence under the PDPO.</td>
<td>1 September 2020</td>
<td>US Department of the Treasury press release dated 7 August 2020</td>
</tr>
<tr>
<td>The PCPD published a case note on whether audio-recording without consent would contravene the requirements of the PDPO</td>
<td>In a recent case note published, the PCPD has stressed that PDPO is principle-based and technology-neutral, and does not prohibit audio-recording. Generally speaking, whether audio-recording is subject to the PDPO depends on whether the act involves collection of personal data. The test is whether it is reasonably practicable to directly or indirectly ascertain the identity of an individual from the recording, or whether the recording party does not intend to compile any information about a specific individual. If the answer is negative, then there will be no collection of personal data, accordingly, neither will the PDPO be applicable under this circumstance, and vice versa. The case note further provides that, although the PDPO does not require that the data subject’s consent must be secured before the collection of personal data can take place, the data user shall collect adequate, but not excessive, personal data by fair and lawful means, and inform the data subject of the purpose of collection. However, certain exceptions under the PDPO apply to the general requirement of giving such notice, for example, when the data is collected for prevention or detection of crime/ unlawful</td>
<td>1 September 2020</td>
<td>Case Note</td>
</tr>
</tbody>
</table>
or seriously improper conduct by persons; (where giving notice would be likely to prejudice these aims).

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
</table>
| The SFC issued a circular to licensed corporates upon review of internet trading cybersecurity (the "Circular") | The Circular was published following SFC’s recent thematic review of selected internet brokers which provide online trading services on desktop, mobile or designated website platforms with a focus on cybersecurity issues and vulnerabilities associated with mobile trading applications. A report to the thematic review was issued on the even date which contains, among other things, deficiencies, instances of non-compliances in many practical areas, and reminders of other requirements (the “Report”). | 23 September 2020 | The Circular  
The Report |
Development | Summary | Date | Links
--- | --- | --- | ---
Resolutions of the NADP on data processing related to "rich lists" and the expression of freedom | Fines totalling HUF 4,500,000 (approximately EUR 12,500) have been imposed on Forbes Hungary, a newspaper which publishes an annual list of the wealthiest Hungarians. The Authority found that Forbes did not properly consider the relevant interests in connection with the publication. It also failed to inform the relevant data subjects in advance about its own and third party (public) legitimate interests, as well as the results of its comparison between those interests and the interests of the data subjects. The Authority highlighted that even in the case of business journalism, if data controllers wish to use legitimate interest as a legal basis, a balance of interests should be carried out in accordance with the GDPR (and this includes a second, individual balance of interests after any objection by the relevant data subjects). However, The Authority also considered the principle of the freedom of press in the context of data subjects’ rights and in this case refused the applicant’s request to have their personal data erased. | 23 July 2020 | Full NADP resolution 2020/1154 (in Hungarian)  
Full NADP resolution 2020/838 (in Hungarian)

Resolution of the NADP on the violation of the obligation to provide information and the | The Authority found that Google Ireland has violated data subjects’ right of information and access by failing to provide adequate information on the processing of the data subjects’ | 16 July 2020 | Full NADP resolution (in Hungarian)
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>exercise of the rights of data subjects residing in Hungary in connection with the Google AdWords service</strong></td>
<td>personal data (name, in this context) in the context of Google AdWords. However, the Authority found no evidence of a systematic problem in this respect and for this reason it deemed that the involvement of the Irish Data Protection Authority was unnecessary.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marie McGinley</td>
<td>Partner</td>
<td>T: +35 31 64 41 45 7 <a href="mailto:mariemcginley@eversheds-sutherland.ie">mariemcginley@eversheds-sutherland.ie</a></td>
</tr>
<tr>
<td>Neasa Ní Ghráda</td>
<td>Senior Associate</td>
<td>T: +35 31 66 44 25 8 <a href="mailto:neasanighrada@eversheds-sutherland.ie">neasanighrada@eversheds-sutherland.ie</a></td>
</tr>
<tr>
<td>Kirsty Farrell</td>
<td>Solicitor</td>
<td>T: 35 3 1 66 449 41 <a href="mailto:KirstyFarrell@eversheds-sutherland.ie">KirstyFarrell@eversheds-sutherland.ie</a></td>
</tr>
</tbody>
</table>

## Ireland

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>The DPC publishes statement on Schrems II decision</td>
<td>In this blog post, the Data Protection Commission (&quot;DPC&quot;) discusses the Schrems II judgment (which it 'strongly welcomes'), including (amongst others) discussion of why it commenced the proceedings in this case.</td>
<td>16 July 2020</td>
<td>DPC Guidance</td>
</tr>
<tr>
<td>DPC publishes guidance on processing Customer Data for COVID-19 Contact Tracing</td>
<td>The DPC has provided guidance to businesses to help them maintain records of customers who have visited their business while also keeping this personal data safe. It also guides businesses on how to navigate data protection obligations to protect clients’ and visitors’ privacy rights whilst following government advice designed to help keep individuals safe.</td>
<td>14 September 2020</td>
<td>DPC Guidance</td>
</tr>
</tbody>
</table>
On 6 July 2020 the Italian Data Protection Authority ("IDPA") updated its previously issued FAQs on COVID-19, addressing schools, employers, health care, research, local authorities and providing clarification and guidance for public and private bodies. With reference to the usage of contact tracing apps in the context of private undertakings, IDPA specified that currently the contract tracing function is only regulated by art. 6, of the Italian Law Decree n. 28 of 30 April 2020. This provision regulates the Italian Covid-19 alert system to which is connected the app ‘Immuni’, managed by the Italian Ministry of Health.

The IDPA underlined that employers can use apps that do not imply processing of personal data referring to identified or identifiable data subjects in order to reduce contagion risks (e.g. systems anonymously counting the number of persons entering in an identified place and sending an alert/flashing a red light in if the number of these persons is beyond a pre-identified threshold).

On 13 July 2020 the IDPA issued a press release, referring to its updated FAQs on Covid-19, specifying that Italian Regions cannot oblige persons to download tracing apps and that no detrimental consequence can result from failure to install such apps.

With reference to the Immuni app, the IDPA remarked that its installation is voluntary and that no detrimental consequence can result from failure to install such app.

It also stated that the use of telemedicine apps by healthcare organisations does not need a specific consent from the data subject.
### Development Summary

The IDPA also made clear the need for data minimization and care in case of transfers of personal data outside the EU.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDPA issued a press release regarding contact tracing apps</td>
<td>The IDPA issued a short press release on the “proliferation of contact tracing apps by public entities and private subjects”. The IDPA stated that the Covid-19 emergency status is not itself automatically and per se a sufficient legal basis to affect rights and freedoms protected under the Constitution and to allow particularly invasive processing activities of personal data (such as contact tracing). IDPA remarked that currently the only processing activities of personal data which have an appropriate legal basis are those grounded on a national legal provision. Any other processing activity aiming at contact tracing would be groundless and thus in breach of EU and Italian Data Protection law.</td>
<td>10 August 2020</td>
<td>IDPA's press release</td>
</tr>
<tr>
<td>IDPA's measures to fine telecommunication operators</td>
<td>The IDPA issued a press release regarding fines imposed on certain Italian telecommunication operators. In summary: - THE IDPA deemed a leading Italian telecommunication operator liable of multiple data protection violations, mostly related to marketing activities, and fined such operator of almost EUR 17 million (measure n. 143 of 9 July 2020). The IDPA received complaints from the operator's users about unsolicited marketing communications made without their consent via several means. The IDPA reported that in several cases complainants had declared they had not been enabled to exercise their right to withdraw consent or to object to the processing of their data for marketing purposes, partly on account of the inaccurate contact information provided in the information notices. The IDPA also reported that in other cases, users’ personal data had been included in public phone listings despite the objections (also reiterated) made by those users. The IDPA's investigation revealed that the operator's apps had been configured so as to require the user to consent, on each access, to processing activities for various purposes including marketing, profiling, communication of data to third parties, data enrichment and geolocation. The possibility to withdraw such consent was only allowed after 24 hours. The IDPA also commented on</td>
<td>Date of press release: 9 July 2020  Date of IDPA's measures: 9 July 2020</td>
<td>IDPA's press release  IDPA's measure n. 143 of 9 July 2020 (only available in Italian language)  IDPA's measure n. 144 of 9 July 2020 (only available in Italian language)  IDPA's measure n. 138 of 9 July 2020 (only available in Italian language)</td>
</tr>
</tbody>
</table>
the risky nature of processing activities of personal data for marketing purposes. In such respect, the IDPA noted that although the operator adopted some measures, it lacked control of its business partners involved in marketing campaigns, its business partners' subcontractors and the actual compliance of these business partners and subcontractors with the measures adopted. This lack of control in the supply chain was deemed by the IDPA as a breach of the data controller’s accountability principle.

- the IDPA fined a business partner of the operator (see the point above) with a separate but connected proceeding for an amount of EUR 200,000 (see the IDPA’s measure n. 144 of 9 July 2020). The IDPA found that this business partner subcontracted – (not in accordance with the GDPR) whole sets of processing activities to call centres, which collected data in breach of the law

- the IDPA fined another telecommunication operator for an amount of EUR 800,000 (see IDPA’s measure n. 138 of 9 July 2020). The IDPA reported that this operator was in breach of data protection law in a number of respects, in particular concerning specific telecommunication operators’ obligations of security and regarding employees’ access to traffic data. The operator was also warned by the IDPA

**IDPA's measure on the requirements for the accreditation of monitoring bodies**

On 9 July 2020 the IDPA issued a press release, announcing its measure n. 98 of 10 June 2020 on the requirements for the accreditation of monitoring bodies under art. 41 GDPR. This accreditation of the monitoring bodies is necessary for the approval of a code of conduct pursuant to art. 40 GDPR. The requirements set forth by the measure include (amongst others): independence and impartiality; documented procedures to prevent conflicts of interest; appropriate level of competence for the correct performance of monitoring tasks; appropriate procedure to assess if controllers and processors can be admitted to the code of conduct and can apply it; and capability of managing in a transparent and impartial manner complaints on the breach of the code of conduct by its members.
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
</table>
| IDPA's measure to establish additional requirements for the accreditation of certification bodies | On 4 September 2020 IDPA issued a press release making available its measure n. 148 of 29 July 2020. This measure provided additional requirements for the accreditation with reference to ISO/IEC 17065:2012 of certification bodies pursuant to article 43, parr. 1 (b) and 3, GDPR. These requirements include the absence of conflicts of interest, appropriate training of human resources, appropriate management of complaints, periodic assessments on services and products certified. The Italian accreditation body is "Accredia" who will assess certification bodies on the basis of the requirements under EN-ISO/IEC 17065:2012 and on the basis of the additional requirements identified by the IDPA. | Date of press release: 10 August 2020  
Date of IDPA's measure: 29 July 2020 | IDPA's press release (only available in Italian language)  
IDPA's measure n. 148 of 29 July 2020 (only available in Italian language) |
Guidelines for the assessment of requests for the provision of personal data have been provided for public consultation

The State Data Protection Inspectorate has prepared and submitted for public consultation guidelines for the assessment of requests for the provision of personal data.

With these guidelines, the Inspectorate aims to help data controllers and data processors better understand how to assess incoming requests for the provision of personal data. For example, whether certain requests for personal data should be fulfilled, the criteria which should be used to assess the lawfulness and reasonableness of requests, the information which must be included in the request, how the controller must ensure confidentiality so that personal data is not disclosed to individuals who have no legal basis for access to the requested personal data.

The draft guidelines submitted for public consultation can be found here (in Lithuanian).

The State Data Protection Inspectorate has announced the 2020 changes to the inspection plan

The State Data Protection Inspectorate carries out planned inspections of enterprises, institutions and other organizations in accordance with its inspection plan which is approved annually. However, the plan may be adjusted during the year (in some circumstances).

On the basis that the Member States of the European Union have an obligation to apply the GDPR consistently and to ensure a uniform level of protection of personal data, and that the public consultations on European Data Protection Board Guidelines 2020/06 on the Second Payment Services Directive (PSD2) and the GDPR have not been completed, the Inspectorate has decided this year to adjust its inspection plan and waive inspections of financial institutions regarding the personal data processed when...
The State Data Protection Inspectorate has published a description of the procedure for approving binding corporate rules ("BCRs")

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>providing a payment initiation service. However, these inspections are planned for next year.</td>
<td>The GDPR regulates the processing of personal data both inside and outside the European Economic Area (&quot;EEA&quot;) and contains specific requirements for that transfers of personal data from within the EEA to outside of the EEA (third countries). One of the permissible grounds under GDPR for such transfers are binding corporate rules (&quot;BCRs&quot;) (for companies within the same corporate group). The State Data Protection Inspectorate has prepared a description of the procedure for approving BCRs, including which documents must be submitted to which data protection supervisory authority to apply for approval of BCRs. In order to transfer personal data on the basis of BCRs, the controller must submit a request, draft BCRs, additional documents justifying the obligations imposed by the BCRs and a table with references to the compliance of the submitted documents with the BCRs approval criteria. All documents must be submitted in English. The application is submitted to the lead supervisory authority, which is determined by the EEA State in which the group has its head office. The data controller must justify in its application for approval why a particular supervisory authority has been chosen as the lead supervisory authority.</td>
<td>21 September 2020</td>
<td>A description of the rules of procedure approved by the Director of the State Data Protection Inspectorate can be found here (in Lithuanian).</td>
</tr>
</tbody>
</table>
### Malaysia

#### Contributors

- **Brian Law**  
  *Regional Head of IP*  
  T: +65 6361 9873  
  brianlaw@law-partnership.com

- **Suaran Singh Sidhu**  
  *Partner*  
  T: +603 9212 9287  
  suaransidhu@law-partnership.com

---

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
</table>
| **Mandatory use of MySejahtera Contact-Tracing Application for travellers entering Malaysia** | By way of background, the “MySejahtera” Application was launched by public authorities for nationwide use in April 2020. The App’s main goal is to allow for a more efficient and streamlined method of contact-tracing amidst the COVID-19 pandemic. Users need only register their details on the App upon downloading, and may then proceed to use the App to scan the MySejahtera QR codes displayed at most storefronts nationwide.  
  
  In July, the Guidelines (Entry and Quarantine Process) for Persons Under Surveillance Returning from Abroad published by the National Disaster Management Agency mandate that all persons entering Malaysia from abroad must download and use the MySejahtera contact-tracing application during their time in Malaysia. Additionally, for persons entering Malaysia, essential information such as travel information (date and time, flight information, and port of embarkation) as well as a health declaration must be registered on the MySejahtera application at least one day from the date of departure to Malaysia. | 24 July 2020 | Guidelines |

---
#### Mauritius

**Contributors**

<table>
<thead>
<tr>
<th>Profile</th>
<th>Name</th>
<th>Title</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Nitish Hurnaum</td>
<td>Partner</td>
<td>T: +230 211 0550 <a href="mailto:nitishhurnaum@eversheds-sutherland.mu">nitishhurnaum@eversheds-sutherland.mu</a></td>
</tr>
<tr>
<td></td>
<td>Yannick Fok</td>
<td>Partner</td>
<td>T: +230 211 0550 <a href="mailto:yannickfok@eversheds-sutherland.mu">yannickfok@eversheds-sutherland.mu</a></td>
</tr>
</tbody>
</table>

## Development Summary

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enactment of the Data Protection (Fees) Regulation 2020</strong></td>
<td>The Data Protection Regulations 2009 have been repealed and replaced by the Data Protection (Fees) Regulation 2020 which came into force on 1 August 2020. All registrations/renewals which were granted prior to 1 August 2020 are, as from 1 August 2020, no longer valid and, as such, all controllers and processors will need to make a fresh registration with the Data Protection Office in order to be compliant with section 14 of the Data Protection Act 2017 (the &quot;DPA&quot;) and the new Regulations. Taking into consideration that some controllers and processors have already renewed their registration for the year 2020, the Data Protection Office is providing a moratorium period of 3 months from 1 August 2020 to all controllers and processors to apply for the new registration. In addition, the fees have been reduced and the registration is now valid for 3 years. Failure to register as controller/processor after the moratorium period may amount to an offence under the DPA and consequently, on conviction, a fine not exceeding 200,000 rupees and imprisonment for a term not exceeding 5 years on conviction may be imposed.</td>
<td>1 August 2020</td>
<td><a href="#">Data Protection (Fees) Regulation 2020</a> <a href="#">DPO Communique</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ratification of the Protocol amending Convention for the Protection of individuals with regard to automatic processing of personal data</strong></td>
<td>Mauritius has signed and deposited, on 4 September 2020, its instrument of ratification of the Protocol amending Convention for the Protection of individuals with regard to automatic processing of personal data (CETS 223).</td>
<td>4 September 2020</td>
<td><a href="#">DPO Communique on ratification of the protocol amending Convention for the Protection of individuals with regard to automatic processing of personal data</a></td>
</tr>
</tbody>
</table>
Mauritius has thus become the 6th State after Bulgaria, Croatia, Lithuania, Poland and Serbia as well as the first country in Africa to ratify the modernised Convention 108 (Convention 108+).

The modernisation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the only existing legally binding international treaty with global relevance in this field, addresses the challenges to privacy resulting from the use of new information and communication technologies, and strengthens the convention's mechanism to ensure its effective implementation.

The Protocol provides a robust and flexible multilateral legal framework to facilitate the flow of data across borders while providing effective safeguards when personal data are being used. It constitutes a bridge between different regions of the world and different normative frameworks, including the GDPR in the European Union which refers to Convention 108 in the context of transborder data flows.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mauritius</td>
<td>Mauritius has thus become the 6th State after Bulgaria, Croatia, Lithuania, Poland and Serbia as well as the first country in Africa to ratify the modernised Convention 108 (Convention 108+). The modernisation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the only existing legally binding international treaty with global relevance in this field, addresses the challenges to privacy resulting from the use of new information and communication technologies, and strengthens the convention's mechanism to ensure its effective implementation. The Protocol provides a robust and flexible multilateral legal framework to facilitate the flow of data across borders while providing effective safeguards when personal data are being used. It constitutes a bridge between different regions of the world and different normative frameworks, including the GDPR in the European Union which refers to Convention 108 in the context of transborder data flows.</td>
<td></td>
<td>automatic processing of personal data (CETS 223) by Mauritius</td>
</tr>
</tbody>
</table>
Netherlands

Development

Summary

Following a request for prior consultation under Article 36 GDPR by the Minister of Health, Welfare and Sport, the DPA indicated that the privacy of users of the Dutch contact tracking app, also known as the 'CoronaMelder' App, is still not sufficiently guaranteed.

The DPA advised that the Minister still needs to conclude additional agreements with Google and Apple regarding the software and the processing of personal data; that legislation should be put in place to properly regulate the use of the App; and that further investigations are needed in order to find out whether the servers that are being used are secure.

The DPA has advised the Minister not to roll out the App until these steps have been taken.

Date
6 August 2020

Links
Publication (in Dutch)

Contributors

Olaf van Haperen
Partner
T: +31 6 17456299
olafvanhaperen@eversheds-sutherland.nl

Robbert Santifort
Senior Associate
T: +31 6 81880472
robbertsantifort@eversheds-sutherland.nl

Judith Vieberink
Senior Associate
T: 31 6 52644063
judithvieberink@eversheds-sutherland.nl

Marijn Rooke
Associate
T: +31 6 30261891
marijnrooke@eversheds-sutherland.nl

Sarah Zadeh
Associate
T: +31 6 81880484
sarahzadeh@eversheds-sutherland.nl
### Development

#### Dutch DPA approves the first Dutch code of conduct based on Article 40 GDPR

On 20 August 2020, the Dutch Data Protection Authority ("DPA") approved the first Dutch code of conduct as referred to in Article 40 GDPR.

It concerns the Data Pro Code of NLdigital, a sector association for the digital sector. The Code offers affiliated IT companies guidelines on how to interpret open standards as mentioned in the GDPR and offers practical documents they can use in their organisation or share with customers. An example is the 'Data Pro Statement', which is a statement that informs potential clients about the guarantees they offer when it comes to the protection of personal data.

A branch or sector that has drawn up a code of conduct can ask the DPA to approve it. The DPA approves a code of conduct if it meets the requirements for a code of conduct as laid down in article 40 GDPR. It is particularly important in this respect that the code of conduct provides a concrete and detailed application of the GDPR. It should not simply restate the relevant provisions of the GDPR.

The organisation that draws up the code of conduct must also supervise the code of conduct by setting up a supervisory body. This body monitors compliance with the code of conduct, assesses whether affiliated parties are eligible to apply the code of conduct and deals with complaints about breaches of the code of conduct.

The DPA must accredit the monitoring body and then assess, among other things, the independence and expertise of the supervisory body.

Like the other European data protection authorities, the DPA must establish criteria for this and submit them to the European Data Protection Board for advice. The Dutch DPA has already done this and expects the outcome before the end of 2020.

**Date:** 27 August 2020  
**Links:** Publication (in Dutch)

---

#### The District Court of Amsterdam rules on DSAR

On 17 September 2020, the District Court of Amsterdam ordered a claimant (a former employee) to pay the court approved scale of costs following the claimant’s withdrawal of his court application.

**Date:** 17 September 2020  
**Links:** N/A
The application concerned a data subject access request ("DSAR"") via the route of Article 36 Dutch GDPR Implementation Act, requesting, amongst others, a full copy of the personnel file. Our Dutch Eversheds Sutherland Data Protection Team assisted the client (a large industrial market player) in this matter, after successful representation in summary proceedings, in which all claims were already rejected in full.

### District Court of The Hague rules that the right of access does not constitute a right to a copy of the documents containing personal data

On 10 August 2020, the District Court of The Hague considered whether a technical university had fully complied with a DSAR on the basis of Article 15 GDPR made by a student. The student (the claimant in this case) had been given a copy of his personal file, with the exception of work notes issued by student advisors. However, he argued that the file was not complete, and that the university did not fully comply with his right of access.

The Court ruled that the right of access does not constitute a right to a copy of the documents containing personal data. It depends on the specific circumstances of the case and on the controller to determine the manner in which access is granted.

Access can be granted by providing an overview of the personal data being processed or by providing a copy. If a copy of documents or records is provided while it is also sufficient to provide an overview of the personal data being processed, an overview of the personal data suffices.

Furthermore, the Court ruled that if the claimant is of the opinion that more personal data is being processed than has been disclosed by the controller, while the controller has carried out an investigation, it is up to the claimant to prove whether more personal data is being processed.

### The Court of Appeal in The Hague rules on request for erasure of credit score based on Article 21 GDPR

On 8 September 2020, The Court of Appeal in The Hague considered whether a leading bank was obliged to remove appellant’s credit score on the basis of the assessment under Article 21 GDPR.

As a result of several overdue payments and after failing to comply with a payment arrangement, the bank had registered the appellant in the Central Credit Information System ("CKI"), which is managed by the Dutch Credit Registration Office ("BKR"). The
claimant requested the bank to remove her credit score from the CKI.

Initially, the District Court of The Hague ruled against the appellant and the appellant lodged an appeal against the District Court’s decision.

The Court of Appeal considered that registration in the CKI constitutes a processing of personal data within the meaning of the GDPR. Pursuant to Article 21(1) of the GDPR, a data subject has the right to object at any time to the processing of data relating to him or her on the basis of Article 6(1) under (e) or (f) of the GDPR for reasons related to his or her specific situation. In the event of an objection by the data subject, the controller must discontinue the processing of the personal data, unless the controller invokes compelling legitimate grounds for the processing that outweighs the interests of the data subject.

In the opinion of the Court, Article 6(1)(f) GDPR provides a basis for the data processing by the BKR. The Court did not find it plausible that the data processing is also necessary to comply with a legal obligation that rests on the bank as controller. The Court therefore assumes Article 6(1)(f) GDPR should be considered as the legal ground for the lawful processing of personal data and the appellant has a right to object the processing. However, the Court ruled that the appellant did not have a pressing need or overriding interest, as she only wanted to take out an additional mortgage in order to divide her house in separate apartments. The Court thus ruled that the bank was not obliged to remove her (negative) credit score.

The Court of Appeal in Den Bosch rules that the Dutch Credit Information System has a legal basis and constitutes a legal obligation to process personal data

On 6 August 2020, the Court of Appeal in Den Bosch considered whether the BKR had to remove the credit score from the appellant from the CKI, which is managed by the BKR.

For a certain period of time, the appellant was seriously ill and his partner did not have a job. The appellant was self-employed and was not insured against incapacity for work. Consequently, there was no income and debts increased. For this reason, the appellant received a negative credit score. Although the credit score will be removed in March 2021, the appellant wanted this to happen sooner because he was unable to take out new loans.
Initially, the Court of Zeeland-West-Brabant ruled against the appellant and the appellant logged an appeal against the Court’s decision.

The Court of Appeal of Den Bosch considered whether the credit registration system in The Netherlands has a legal basis and therefore constitutes a legal obligation to process personal data, also within the meaning of article 6(1)(c) GDPR. The DPA previously (and remarkably) concluded in a letter to the Minister of Finance of 14 November 2019 that there was no such legal basis.

However, the Court concluded that the credit registration system in The Netherlands has a legal basis and consequently data controllers such as credit institutions and banks can therefore rely on Article 6(1)(c) GDPR as a basis for the processing operations. In its judgment, the Court expressly stated that private parties can also rely on the basis of Article 6 (1)(c) GDPR and that a legal basis specifically designed for each processing activity is not required. The Court even explicitly stated that it does not share the view of the DPA.

The fact that there is a legal obligation and therefore a legal basis for processing does not detract from the fact that the requirements of proportionality and subsidiarity must be met in the specific case. The Court was of the opinion that these requirements have been met. The duration of the registration is five years and that duration is proportional according to the Court. The negative credit score will therefore not be removed before March 2021.

The Court of Appeal rules on (legitimate) employee privacy breach

On 27 July 2020, the Court of Appeal in Arnhem-Leeuwarden considered whether an employer had violated the privacy of an employee.

The employer instructed a corporate investigator to investigate the possible absenteeism fraud by an employee who was on sick leave with a hernia. The investigator observed the employee for half a day from a car parked on the public road. The employee was fired on the spot, because she appeared to work in her own tea garden, as shown by the observation. In court proceedings in
first instance, the employee claimed damages from the investigator for violation of her privacy.

The District Court dismissed her claim and the Court of Appeal upheld this judgment. It was ruled that the observation by the investigator constituted a breach of the employee's privacy, but in this case the breach was legitimate. After all, the investigator had acted in accordance with the Privacy Code of Conduct for Private Research Agencies and this code has been (prior to the GDPR) approved by the DPA.

The Dutch DPA imposes a fine on the Dutch Credit Registration Office ("BKR")

The Dutch DPA imposed a fine of €830,000 on the BKR due to non-compliance with Articles 12(2) and 12(5) of the GDPR from May 2018 until March 2019. The BKR registers loans and debts of consumers in the Netherlands, calculates the credit scores of consumers and provides third parties on request with information regarding the creditworthiness of consumers.

In May 2018, the BKR began charging a fee to data subjects for requesting access to their personal data in a digital format. Although data subjects could obtain a free paper copy of their data, this was only possible once a year. After the DPA received multiple complaints from data subjects about the difficulties involved in accessing their personal data and the applicable fees, the DPA started investigating this matter.

The DPA concluded that the BKR had infringed Articles 12(2) and 12(5) of the GDPR by charging a fee to data subjects that wanted to access their personal data in a digital format and by (actively) discouraging data subjects from filing a data subject access request. The DPA stressed that it is important for data subjects to access their credit registration data, as a negative credit registration will have far-reaching consequences for individuals. Following the investigation of the DPA, the BKR has modified its data subject access procedures.

Dutch Tax and Customs Administration violates the GDPR and Dutch Data Protection Act

Following a signal received in April 2017 about the possible processing of the dual nationality of applicants for childcare benefits by the Benefits Department of the Tax and Customs Administration, the DPA initiated an investigation. During the investigation, the DPA made four written requests for information and documents from the Department. In addition, the DPA
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>requested information from the National Audit Service and took statements from the director and several (former) employees of the Department.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The report mentions that the Department should have deleted data on dual citizenship in January 2014. However, in May 2018, 1.4 million dual citizens were still registered within the system and, although dual nationality does not play a role in assessment of childcare benefits applications, the data was retained and used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Furthermore, the Tax and Customs Administration also processed the nationality data of the applicants for the purpose of combating organised fraud, even though this data was not necessary for this purpose. Lastly, the Tax and Customs Administration used the nationality of the applicants (Dutch/not Dutch) as an indicator to automatically designate certain applications as 'high risk'.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The DPA concluded that these practices was unlawful and discriminatory, and that the Minister of Finance, as data controller, violated:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>− the principle of lawfulness laid down in Article 5(1) GDPR in conjunction with Article 6(1) GDPR, and Article 6 Dutch Data Protection Act in conjunction with Section 8 of the Dutch Data Protection Act; and</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>− the principle of fairness, laid down in Article 5(1)(a) GDPR and Article 6 Dutch Data Protection Act.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The DPA is currently awaiting an official response of the Minister of Finance. After receiving this response, the DPA will determine whether a sanction will be imposed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Contributors

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

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

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

---

**Development** | **Summary** | **Date** | **Links**
--- | --- | --- | ---
Fines for the illegal disclosure of restricted information are planned to increase tenfold | State Duma deputies have developed amendments to the Russian Code of Administrative Offenses, which were also supported by the Russian Government. It is proposed to increase liability for committing an administrative offence in relation to the disclosure of information, access to which is limited by law (if such disclosure does not entail criminal liability), by a person who has received such access in connection with the performance of official or professional duties. Currently the sanctions for committing such an offense provides for an administrative fine for individuals in an amount between RUB 500 and 1,000, and for officials, the fine is between RUB 4,000 and 5,000. However, the amendments propose increasing the fines for citizens to between RUB 5,000 and 10,000, and for officials, to between RUB 40,000 and 50,000. | 31 July 2020 | Text of the Bill (in Russian)

The Law on Experimental Legal Regimes for Digital Innovation was adopted and signed | Legal entities developing digital technologies will now have the opportunity to use experimental legal regimes after the Law on Experimental Legal Regimes for Digital Innovation was adopted and signed (the so-called "Regulatory Sandbox"). The intention is to reduce costs and the amount of time necessary to introduce innovative products, reduce legal risks, accelerate the launch of | 31 July 2020 | Text of the Law (in Russian)
new solutions on the market, and filter out ineffective business models.

The Regulatory Sandboxes assume specific experimental regulation for its participants (and supersedes or supplements other regulations that would apply) for up to three years, with the possibility of extension for one additional year.

The primary goal of the document is to create legal conditions for the accelerated emergence and implementation of new products and services in the areas of the application of digital innovations using digital technologies, such as artificial intelligence, a distributed ledger (blockchain), neurotechnology, quantum technologies and others according to the list determined by the government.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
</table>

| new solutions on the market, and filter out ineffective business models. The Regulatory Sandboxes assume specific experimental regulation for its participants (and supersedes or supplements other regulations that would apply) for up to three years, with the possibility of extension for one additional year. The primary goal of the document is to create legal conditions for the accelerated emergence and implementation of new products and services in the areas of the application of digital innovations using digital technologies, such as artificial intelligence, a distributed ledger (blockchain), neurotechnology, quantum technologies and others according to the list determined by the government. | | | |
Spain

Contributors

Juan Díaz
Managing Partner
T: +34 91 429 43 33
jdiaz@Eversheds-sutherland.es

Vincente Arias Máiz
Partner
T: +34 91 429 43 33
varias@eversheds-sutherland.es

Celia Bouzas González
Senior Associate
T: +34 91 429 43 33
cbouzas@Eversheds-sutherland.es

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Spanish Government passes the Royal Decree-Law 28/2020 of 22 September on remote working (&quot;Teleworking Law&quot;)</td>
<td>The new Teleworking Law includes some references to data protection in the context of remote working that is carried out with the exclusive use of computer, telematic and/or telecommunication means:</td>
<td>23 September 2020</td>
<td>Teleworking Law (in Spanish)</td>
</tr>
<tr>
<td></td>
<td>− a telework agreement must be formalised between the employer and the employee, which shall contain the instructions issued by the employer regarding data protection and information security specifically applicable to distance work. The employer must provide a copy of these agreements to the employee's legal representatives (excluding from these copies information that may affect personal privacy and observing the due protection of the employee's personal data)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>− furthermore, the right to privacy and data protection must be guaranteed in accordance with the principles of adequacy, necessity and proportionality. For example, the employer cannot oblige the use of the employee's personal devices in the performance of remote work or the installation of monitoring and control apps on these work devices owned by the employee</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
the Teleworking Law also emphasises that the employer must preserve the right to digital disconnection (which every employee has and which is developed in the Spanish Organic Law 3/2018 of December 5, on the Personal Data Protection and guarantee of Digital Rights)

− employers must establish criteria for the use of digital devices (the legal representation of employees shall participate in establishing these criteria). In all cases, the minimum standards of protection of privacy must be respected in accordance with social customs and legally and constitutionally recognised rights; and

− collective labour agreements may specify the terms under which employees may use the computer equipment provided by the employer for distance working, for personal use, considering social practices and the specific nature of this type of work

The AEPD issues a notice on the collection of personal data by establishments aimed to react to possible new outbreaks of COVID-19, by recording certain data on customers who go to leisure premises

The Spanish Data Protection Authority ("AEPD") has clarified that data collected, despite being related to the control of the pandemic and related processing to be able to identify possible infections, are not "special categories of personal data".

In order to keep a record of clients who visit leisure premises, the necessity of the record must be recognised by the health authorities and this processing must be mandatory and determined by law. In this case, the legal bases for processing the personal data would be:

− compliance with a legal obligation; and

− performance of a task in the public interest in connection with the control of the pandemic.

In addition, if consent were used as the legal basis, it would be necessary that no negative consequences were derived, that is, that entry to the premises is not prevented.

It would be necessary to justify that there are no other more moderate measures with equal effectiveness for the achievement of the intended purpose. For this reason these measures should be clearly identified and limited to those places where there is greater difficulty in complying with these measures (a nightclub,
in which people want to be close, is not the same as a museum, in which suitable spaces can be provided for people to circulate and limit contacts to a great extent. According to the AEPD criteria, it should be up to the health authorities to make a reasoned assessment of where identification would be mandatory.

Customers should also receive clear, simple and accessible information about the processing before the personal data are collected and the information collected must be processed with the appropriate security measures.

The AEPD updated its Guide on the use of cookies to adapt it to the new guidelines of the EDPB

The European Data Protection Board ("EDPB") revised in May 2020 the Guidelines 05/2020 on consent in order to clarify its position on two issues: the validity of "scrolling or swiping through a webpage" option as a way of providing consent by users and the possibility of using so-called "cookie walls", i.e. limiting access to certain services or content only to users who accept the use of cookies.

Accordingly, the AEPD has updated its Guide on the use of cookies ("Guide") in response to these clarifications, in particular:

- the Guide explains that so-called "cookie walls" that do not offer an alternative to consent cannot be used. This is particularly important in those cases where denial of access would prevent the exercise of a legally recognised right of the user, for example, access to a website being the only means provided to the user to exercise such a right; and

- there may be certain cases in which non-acceptance of the use of cookies prevents access to the website or the total or partial use of the service, provided that the user is properly informed and an alternative way of accessing the service without accepting the use of cookies is offered. Moreover, the services provided by such alternative means must be genuinely equivalent, and furthermore it is not valid that the equivalent service is offered by an entity other than the publisher of the relevant website.

These new criteria must be implemented no later than 31 October 2020.
The Spanish Government passes the Organic Law 1/2020 of 16 September on the use of data from the Passenger Name Record for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes ("Law on the use of PNR data")

The Law on the use of PNR data implements the Directive (EU) 2016/681 (of 27 April 2016) on the use of passenger name record data ("PNR") for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Its relevant data privacy provisions are as follows:

- It will enter into force on the 17 November 2020 and will oblige airlines to disclose the data of millions of air travellers with police databases by using electronic means which shall offer sufficient guarantees with regard to the technical security and organisational measures governing the data processing.

- The Law on the use of PNR data will apply to people travelling on international flights, both within and outside the European Union, when they leave or arrive in Spanish territory or make a stopover there.

- The PNR data would include, for example, identification, date of reservation, travel itinerary and method of payment of the ticket, but under no circumstances will the Passenger Information Unit ("PIU") process PNR data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union or political party membership, health, life or sexual orientation.

- The PIU shall appoint a person as PNR data protection officer.

- The authorities shall store PNR data for a maximum period of five years. It is also foreseen that the data must be anonymised within six months of being disclosed by airlines; and

- The purpose for the processing of PNR data is limited to the investigation of serious crimes such as terrorism, drug trafficking or human trafficking, so they cannot be used for more general police investigations. The access to the PNR data is very restricted and can only be requested by the Spanish Civil Guard, the police, the Spanish National Intelligence Centre, the public prosecutor's office and the customs authorities.
**Swedish Government: Name change of the Swedish DPA**

On 21 September 2020, the Swedish Government presented its budget bill for 2021. Among other things it is proposed that the Swedish Data Protection Authority ("DPA") changes name from Datainspektionen to Integritetsskyddsmyndigheten (En. Authority for protection of privacy). The new name is proposed to apply from 1 January 2021.

**Swedish DPA: new guidance on controllers and processors**

The Swedish DPA summarised its guidance on controllers and processors and the concepts of these roles which was recently published by the European Data Protection Board ("EDPB") and made available for public feedback.

In short, the guidance focuses on the determination of the roles as controllers and processors and the consequences of having such role as well as necessary content in a data processing agreement governing the relationship between a data controller and its data processor.

Further, the guidance clarifies the roles as joint controllers and how responsibility is shared between joint controllers.

**Swedish Police: AI to be used to analyse material in ongoing investigations**

The Swedish Police want to use automated image analysis as a tool in investigations. The Police state that video recordings are more and more frequently part of the material used during an investigation, and that automated image analysis will enable a more efficient process to analyse video recordings and for example vehicles, clothes, weapons or even faces or license plates shown in the video recordings. Currently, the police analyse all such material manually which consumes a lot of time and resources.
A pilot programme performed by the Police shows that the use of this technology would lead to shorter processing time, improved quality of the result of the analysis and an improved work environment for administrators. Furthermore, it showed that it would result in improved protection for personal privacy when fewer people, vehicles etc. are processed by administrators. There would also be a positive impact for suspects as they may be dismissed as suspects faster with a more efficient process of analysing material during an investigation.

Since the use of this technology would include processing of sensitive biometric data, the Police requested a prior consultation with the DPA and, following this consultation, the DPA approved the use of this technology. It was found that the Police has a legitimate interest to use this technology but, considering the level of sensitivity of the data processed, the DPA provided written guidance to be followed by the Police prior to initiating use of the technology.

In addition, the Police will on a case by case basis perform an assessment to ensure that the use of the technology is strictly necessary. The Police will also have adequate technical and organisational security measures in place to minimise the risk of a breach of the privacy of people involved.

It should be noted that the technology is not connected to any real time CCTV and will not be run jointly with other records held by the Police.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tetra Pak’s Binding Corporate Rules approved by the DPA</td>
<td>The DPA approved Tetra Pak’s Binding Corporate Rules (“BCRs”). The aim of BCRs is to facilitate the transfer of personal data to group companies outside of the EU/EEA. Tetra Pak group’s BCRs are the first to be approved by the DPA under the GDPR. Before the approval of the BCRs, both the DPA and its sister authorities in relevant countries evaluated and analysed Tetra Pak’s application and the proposed BCRs. In addition, the EDPB issued an opinion on the Binding Corporate Rules prior to the approval.</td>
<td>18 August 2020</td>
<td>DPA Press Statement (In Swedish) EDPB Opinion</td>
</tr>
</tbody>
</table>
### Sweden

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data breach: fake emails have been sent from employees of the Swedish Police and a Swedish bank</strong></td>
<td>Binding Corporate Rules are one of the means that may be used to ensure an adequate level of protection of personal data when transferring it to countries outside of the EU/EEA. To have approved Binding Corporate Rules in place will, consequently, facilitate the transfer of personal data within a group of companies. It has been reported that fake emails have been sent from people working for the Swedish Police as well as a Swedish bank. The emails were sent as an attempt to make the recipient install the trojan NanoCore. The group behind the attacks was identified as a group referred to as TA2719, specialising in tailoring NanoCore attacks in different languages. The emails were tailored so that they would fit the sender. The emails sent from the bank included information on a payment to be made and requested the recipient to confirm payment details. The emails from the Police requested the presence of the recipient as part of an ongoing investigation and a request to review an attachment. Most recipients were real estate brokers and companies in the finance industry. The emails included an attached .iso document that would install the trojan NanoCore and enable the hacker to take control of the infected system and steal sensitive data such as passwords and documents.</td>
<td>11 August 2020</td>
<td>[News article (In Swedish)]</td>
</tr>
</tbody>
</table>

| **Data breach: food delivery service has been subject of a hacker attack** | It has been reported that a food delivery service has been the subject of a hacker attack. The delivery service’s database was hacked and included information on 25,000 Swedish customers and in total approximately 480,000 customers in other countries such as France and Germany. Swedish customers have been informed and the data breach has been reported to German authorities as the lead authority (the food delivery service being is owned by a German company). | 15 July 2020 | [News article (In Swedish)] |
## Development

### Schrems II decision adopted in Switzerland

In September 2020, the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") re-evaluated the level of data protection provided by the Swiss-U.S. Privacy Shield and adopted the so-called **Schrems II** judgement. According to the FDPIC’s re-evaluation, the Swiss-U.S. Privacy Shield does not guarantee an adequate protection level for personal data transferred from Switzerland to the U.S. The FDPIC also mentioned that model clauses (such as the Standard Contractual Clauses), other types of data transfer agreements or binding corporate rules ("**BCRs**") do not automatically guarantee an adequate level of data protection in the recipient third country. According to the FDPIC, it is necessary to assess the risks for the personal data transferred to the third country and to evaluate whether the data transfer agreement – whether based on model clauses or not – or the BCRs provide a sufficient protection against these risks, taking into consideration the access that authorities of the recipient country may have to the transferred personal data and the possibilities to defend against such access. If the data transfer agreement or the BCRs cannot guarantee an adequate protection level, the company has to implement additional safeguards, such as encryption, or refrain from transferring personal data.

These conclusions of the FDPIC are not binding and do not affect the validity of the Swiss-U.S. Privacy Shield. It is, however, unlikely that a court would come to a contrary conclusion in this regard. Companies can therefore no longer rely on the Swiss-U.S. Privacy Shield. They should re-assess the legal basis for data transfers if the transfer personal data to the U.S. is based on the Swiss-U.S. Privacy Shield, but also if they transfer personal data.
## Development

<table>
<thead>
<tr>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>to the U.S. or other third countries based on data transfer agreements or BCRs.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### New Data Protection Act adopted

On 25 September 2020, the new Swiss Data Protection Act was (finally) adopted. The new Act is subject to a 100-day referendum period. Provided that no referendum is held, the Swiss government will determine the date of entry into force of the new Act after the expiry of this period. It is anticipated that the new Act will enter into force between June 2021 and January 2023 (unless a referendum is held).

The new Act does not align exactly with the GDPR, but rather it contains a gradual alignment with GDPR. The most important changes set out in the draft are:

- the introduction of an obligation to maintain a record of processing activities, equivalent to Article 30 GDPR
- the enhancement of the existing duty to inform the data subject when their personal data is collected. This duty to inform will be drafted is similar to the duty found in Articles 13 and 14 GDPR
- the introduction of an obligation to conduct a data protection impact assessment, similar to Articles 35 and 36 GDPR
- the introduction of an obligation to report data breaches. However, this provision will be less strict than the obligation provided by Articles 33 and 34 GDPR
- the limitation of the definition of the term ‘data subject’ to include only individuals (please note that under current legislation, other legal entities are also considered to be data subjects)
- the increase of the maximum fine amount for infringements of the data protection act to CHF 250,000. Unlike the GDPR, this fine can only be imposed to the responsible individuals. However, if it would require disproportionate efforts to identify the responsible individual, a fine of up to CHF 50,000 could be imposed to the company in lieu thereof

Notwithstanding the intended gradual alignment with GDPR, there will still be differences between the Swiss data protection...
legislation and GDPR. For example, the new Act will retain the principle that processing of personal data is in general permitted and only requires a justification under certain circumstances. Also under Swiss law, the data subject’s access right is limited by the data controller’s right to refuse, restrict or defer the provision of the requested information, unlike under GDPR.

The new Act will be accompanied by an ordinance, whose content is not yet known.
## Development Summary

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ICO issues initial statements following Schrems II decision</strong></td>
<td>In the ICO’s statement on 27 July following the Schrems II decision and FAQs from the European Data Protection Board (&quot;EDPB&quot;), it advised companies to: &quot;...take stock of the international transfers you make and react promptly as guidance and advice becomes available. The EDPB has recommended that you must conduct a risk assessment as to whether SCCs provide enough protection within the local legal framework, whether the transfer is to the US or elsewhere. The receiver of the data may be able to assist you with this.”</td>
</tr>
</tbody>
</table>
| **Data protection and Brexit: doubts as to whether any adequacy decision between the UK and the EU will be agreed** | Following the eighth round of Brexit negotiations, the EU's Head of UK Task Force and lead negotiator Michel Barnier issued a statement which noted that the parties have yet to reach a consensus on the necessary guarantees to protect citizens’ fundamental rights and personal data.  
EU officials are considering the UK’s data protection regime to decide whether or not EU data can be transferred to the UK after Brexit under an adequacy decision.  
If the UK decides to follow a more relaxed data protection regime than provided for by GDPR and the EU’s law enforcement directive, EU personal data may be at risk when transferred to the UK. The newly-announced UK ‘national data strategy’ (see update below) has exacerbated concerns as to the UK’s approach to data protection from 1 January 2021. There are further concerns that the UK-US data transfer agreement could lead to the data of EU citizens not being adequately protected if transferred onwards from the UK to the US.  
In making a final decision on adequacy, the EU will require an opinion from the EDPB and the agreement of the member states. |

**Date** | **Links** |
<p>| 27 July 2020 | <strong>Statement</strong> |
| 10 September 2020 | <strong>Statement</strong> |</p>
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK Government admits failure to carry out DPIA on COVID-19 Test &amp; Trace Programme</td>
<td>In a letter responding to the Open Rights Group, the UK Government admitted that it did not undertake a Data Protection Impact Assessment (&quot;DPIA&quot;) before launching its COVID-19 NHS Test &amp; Trace Programme (although see below in relation to a subsequent DPIA in respect of the NHS Test and Trace App).</td>
<td>15 July 2020</td>
<td>Letter</td>
</tr>
<tr>
<td>Department of Health and Social Care issues guidance on NHS Test and Trace App’s DPIA</td>
<td>The Department of Health and Social Care (&quot;DHSC&quot;) has issued guidance (the &quot;Guidance&quot;) on the NHS Test and Trace App’s Data Protection Impact Assessment (the &quot;DPIA&quot;). The DHSC acknowledges the importance of providing assurance and formally documenting how the App functions and protects the privacy and data of individuals. The Guidance acknowledges key functionalities of the App which preserve an individual’s privacy – e.g. user identities will remain anonymous, the App will collect the minimum amount of data required and any processing outside the ambit of the DPIA will be subject to a separate impact assessment. In addition, the Guidance notes that there are certain features of the App which can be disapplied – such as the venue check-in function which involves users scanning a QR code each time they attend a particular venue. Users also have the option (but are not obliged to) enter their symptoms.</td>
<td>13 August 2020</td>
<td>Guidance</td>
</tr>
</tbody>
</table>
| ICO publishes guidance on businesses required to collect customer details for track and trace | The ICO has issued guidance for businesses which, by law, have to collect customer details for the purposes of track and trace. The ICO sets out that this should be a simple process with 5 steps to consider:  
  - only the specific information required by Government guidance should be collected;  
  - businesses should be “clear, open and honest” about how the personal data collected will be used;  
  - data should be kept secure;  
  - data shouldn’t be used for purposes other than track and trace; and  
  - personal data should be erased or disposed of in line with Government guidelines (usually after 21 days). | | Guidance |
<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICO sets regulatory approach in light of the continuing COVID-19 situation</td>
<td>The ICO has updated its ICO’s regulatory approach in light of COVID-19, stating that it will continue to act proportionately and will (when investigating non-compliance with data protection laws) consider amongst other factors whether the non-compliance is as a result of the COVID-19 pandemic. The ICO will continue to support organisations in their approach to data protection – guidance is scheduled to be published on data sharing and accountability, and targeted information for SMEs.</td>
<td>24 September 2020</td>
<td>Letter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Updated regulatory approach</td>
</tr>
<tr>
<td>Sir Brian Leveson appointed as Investigatory Powers Commissioner under UK-US Data Access Agreement</td>
<td>Sir Brian Leveson has been appointed as Investigatory Powers Commissioner to exercise oversight over UK’s use of the UK-US Data Access Agreement due to come into force later this year. The Agreement allows UK authorities to request electronic data necessary for law enforcement purposes directly from US telecommunications companies through a court approved order. Agencies utilising its Agreement powers are required to adhere to and maintain high standards of data protection. Sir Brian Leveson’s role is therefore to exercise oversight over UK authorities’ proper exercise of Agreement powers.</td>
<td>6 July 2020</td>
<td>Press release</td>
</tr>
</tbody>
</table>
| ICO updates resources for organisations in readiness for the end of the Brexit transition period | The ICO has updated its resources for organisations in readiness for the end of the Brexit transition period. The resources have a particular focus on how to prepare if there is no adequacy decision in respect of the UK at the end of the transition period and they include specific guidance for:  
  - large businesses and organisations and data protection specialists;  
  - SMEs; and  
  - police forces and other law enforcement authorities.  
These specific guidance notes are also supplemented by a Frequency Asked Questions note which provides more general guidance on the impact of the end of the transition period on data protection. | Announced 27 July 2020 | Announcement Resources |
### Australia and UK ICOs jointly investigate the use of ‘scraped’ data

The Office of the Australian Information Commissioner and the UK’s ICO have combined to launch a joint investigation into a leading technology company’s facial recognition software. Together they are reviewing the company’s handling of personal data, particularly in respect of the use of ‘scraped’ data and an individual’s biometrics. The company’s facial recognition app allows social media users to upload photos of an individual and match it with other photos from the internet which the company has taken from other social medial sites and web pages.

**Date:** 9 July 2020

**Links:** [Press release](#)

### ICO and Surveillance Camera Commissioner issue statements on Police’s use of facial recognition software

The Information Commissioner’s Office (“ICO”) and Surveillance Camera Commissioner (“SCC”) have both issued statements on the use of facial recognition software, following a court decision which found the Police force in question’s use of automated facial recognition technology to be in breach of human rights and data protection laws. The ICO welcomed the decision as an important step in providing clarification on the use of the technology in public places and commented that there needs to be a clear legal framework in order for the public to have trust and confidence in the police. According to the ICO, the decision can help to achieve that.

The SCC similarly welcomed the decision and commented that it formed the basis of an “evolutionary process” for the development and use of facial recognition technology, but noted for such a process public trust in the technology’s safe and legitimate use is essential. The SCC also appreciated the transparency of the Police during the pilot phase and acknowledged that the decision would be equally beneficial to them. The SCC urged the Home Office to update the Home Secretary’s Surveillance Camera Code of Practice on the basis that the judgement exposed some of its deficiencies which the SCC had identified previously.

**Date:** 11 August 2020

**Links:** [ICO statement](#), [SCC statement](#)

### DDCMS seeks feedback on the representative action provisions of the Data Protection Act 2018

The Department for Digital, Culture, Media & Sport (“DDCMS”) has issued a consultation document (the “Consultation”), seeking feedback from individuals and organisations on the operation of the ‘representative action’ provisions of the GDPR and the DPA.

**Date:** 27 August 2020

**Links:** [Consultation](#)
### Development Summary

<table>
<thead>
<tr>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 July 2020</td>
<td>Guidance</td>
</tr>
<tr>
<td>28 August 2020</td>
<td>Report</td>
</tr>
</tbody>
</table>

#### The representative action provisions allow individuals to appoint relevant non-profit organisations as their representatives to take action on their behalf when their data protection rights have been infringed.

By launching the Consultation, the DDCMS is seeking information on how the provisions are operating in practice and the impact they have had on data subjects, particularly children and non-profit businesses, as well as on organisations against whom representative actions have been taken. The Consultation also seeks views on the introduction of new provisions which would allow non-profits and children’s rights organisations to represent individuals despite not having their authorisation to do so (e.g. representative actions on behalf of children or vulnerable adults).

It is of note that such ‘representative’ actions are a means of bringing so-called privacy ‘class’ actions i.e. litigation claims for a large group of affected data subjects together.

The closing date for responses is 22 October 2020.

#### ICO issues guidance on AI and data protection

In its foreword to the guidance, the ICO flags that the underlying data protection questions for even the most complex artificial intelligence (AI) project are much the same as with any new project that involves the processing or personal data. Whilst it recognises that there are certain aspects of data protection compliance that are more challenging when seeking to implement AI (e.g. data minimisation, transparency and individual rights), the message from the ICO is that these challenges should be surmountable provided that data protection is considered at an early stage.

#### ICO issues report on Business Innovation Privacy Hub

The ICO has issued a report (the "Report") on its Business Innovation Privacy Hub (the "Innovation Hub") which was set up in November 2018 to collaborate with other UK regulators to promote data protection considerations and compliance in the drafting and application of business regulation and thereby provide expert data protection support to a broader range of sectors developing innovative goods and services.

The Report discusses the role and objectives of the Innovation Hub (which the ICO has decided to retain on a permanent basis post its initial funding period), outlines the promotion of privacy
by design and by default as key to the ICO’s approach to good data protection practice, provides examples of case studies where the Innovation Hub has been used in practice, as well as providing a list of ‘top ten tips for innovators’ (also published by the ICO as a blog) to help businesses develop new products at the same time as adopting good data protection standards.

### Accountability Framework launched by ICO

The ICO has launched the beta version of its Accountability Framework (the "Framework") to assist organisations to manage their accountability obligations under data protection legislation. The Framework is divided into ten categories, and includes a self-assessment tool to allow organisations to assess how well they are meeting their accountability obligations.

A survey on the Framework has been opened, and will close on 2 November 2020.

<table>
<thead>
<tr>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 September 2020</td>
<td>Press release Framework Consultation</td>
</tr>
</tbody>
</table>

### ICO’s Age Appropriate Design Code comes into force

The Age Appropriate Design Code (the "Code") was issued by the ICO on 12 August 2020 and came into force on 2 September 2020.

The Code, noted as being the first of its kind, sets out 15 flexible standards of age appropriate design that organisations should adopt to ensure their services sufficiently protect and safeguard children's personal data and process children's personal data fairly.

<table>
<thead>
<tr>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 September 2020</td>
<td>Code</td>
</tr>
</tbody>
</table>

### UK National Data Strategy launched

The Digital Secretary has published a National Data Strategy ("NDS") designed to support the use of data in the UK, particularly to drive the recovery from the Covid-19 pandemic.

The Government’s five ‘priority missions’ are stated as: (1) unlocking the value of data across the economy; (2) securing a pro-growth and trusted data regime; (3) transforming government’s use of data to drive efficiency and improve public services; (4) ensuring the security and resilience of the infrastructure on which data relies; and (5) championing the international flow of data.

A public consultation on the NDS will be open until 2 December 2020.

<table>
<thead>
<tr>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 September 2020</td>
<td>Press release Strategy Consultation</td>
</tr>
</tbody>
</table>
### Development

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMA publishes guidance on using purchased marketing lists</td>
<td>The Data &amp; Marketing Association (&quot;DMA&quot;) has released an article which discusses challenges relating to the use of purchased marketing lists and sets out steps for organisations to follow (which have a common theme of transparency) to enable them to remain compliant with GDPR and the DMA Code. Notably, the article expresses disagreement with the ICO’s view (expressed in the ICO’s draft Direct Marketing Code) that consent is a ‘better’ lawful basis for processing personal data for direct marketing purposes than legitimate interests.</td>
<td>17 September 2020</td>
<td>Article</td>
</tr>
</tbody>
</table>
Recent changes to state data breach notification laws in Indiana, Louisiana, and Virginia

Data privacy and cyber security laws continue to rapidly develop in the United States. In addition to developments in California, there have been updates in Indiana, Louisiana, and Virginia based on the National Association of Insurance Commissioner’s (“NAIC’s”) Insurance Data Security.

Indiana recently enacted Insurance Code Chapter 27, Insurance Data Security, based on the NAIC’s model law. Insurers and other entities licensed by the state’s Department of Insurance will now have to maintain an information security programme, conduct a risk assessment, and maintain an incident response plan. The law also requires insurers to notify the state insurance commissioner within 3 business days after making a determination that a cybersecurity event occurred. The new law came into effect on 1 July 2020.

Louisiana recently enacted Insurance Code Chapter 21, Insurance Data Security, which is also based on the NAIC’s model law.

Effective Date of Indiana H.B. 1372: 7 September 2020
Effective Date of Louisiana H.B. 614: 1 August 2020
Effective Date of Virginia H.B. 1334: 1 July 2020

Links:
- Indiana H.B. 1372
- Louisiana H.B. 614
- Virginia H.B. 1334
## United States

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>United States</strong></td>
<td>Similar to Indiana’s law, insurers and other entities licensed by the state’s Department of Insurance must maintain an information security programme, conduct a risk assessment, and maintain an incident response plan. The law also requires licensed entities to notify the insurance commissioner within 3 business days of a cybersecurity event. The new law came into effect on 1 August 2020. Virginia recently enacted Insurance Code, Chapter 6, Article 2, Insurance Data Security Act, which is also based on the NAIC’s model law. Similar to Indiana’s and Louisiana’s new laws, insurers and other entities licensed by the state’s Department of Insurance must maintain an information security programme, conduct a risk assessment, and maintain an incident response plan. The law also requires licensed entities to notify the insurance commissioner within 3 business days of a cybersecurity event. The new law came into effect on 1 July 2020.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Proposed State of Washington Data Privacy Act released for review and comment</strong></td>
<td>On 9 September 2020, Washington Senator Reuven Carlyle, D-Seattle, announced a version of the Washington Privacy Act 2021 was released for public review, comments and feedback. This is the third draft Washington Privacy Act released within the last three years. The previous versions of the Washington Privacy Act were unsuccessful in passing the Washington House of Representatives. The 2021 version is similar to past drafts, but includes new sections for data privacy regarding public health emergencies related to COVID-19 and the processing of personal information for automated contact tracing.</td>
<td>9 September 2020</td>
<td><a href="#">Washington Privacy Act of 2021</a></td>
</tr>
<tr>
<td><strong>FTC confirms intent to enforce the EU – U.S. Privacy Shield Framework despite European court invalidation; Dept. of Commerce issues White Paper.</strong></td>
<td>On 16 July 2020, the Schrems II decision invalidated the Privacy Shield Framework. Despite this judgment, the FTC indicates that it “continue[s] to expect companies to comply with their ongoing obligations with respect to transfers made under the Privacy Shield Framework.” The FTC also “encourage[s] companies to continue to follow robust privacy principles, such as those underlying the Privacy Shield Framework, and to review their privacy policies to ensure they describe their privacy practices accurately, including with regard to international data transfers.” The Department of Commerce (“DoC”) issued a White Paper responding to the European Court’s decision “to provide a</td>
<td>FTC update on Privacy Shield Framework: 21 July 2020</td>
<td><a href="#">FTC Update on Privacy Shield Framework</a>, <a href="#">Dept. of Commerce White Paper</a></td>
</tr>
<tr>
<td>Development</td>
<td>Summary</td>
<td>Date</td>
<td>Links</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>detailed discussion of [the wide range of information about privacy protections in current U.S. law and practice relating to government access to data for national security purposes], focusing in particular on the issues that appear to have concerned the ECJ.” The White Paper seeks to assist organizations in assessing whether their EU-US data transfers offer appropriate protection in accordance with the ECJ’s ruling.</td>
<td>23 September 2020</td>
<td>U.S. Senate Commerce, Science, and Transportation Committee holds hearing on federal data privacy legislation. On 23 September 2020, the Senate Commerce, Science, and Transportation Committee held a hearing on federal data privacy legislation. The hearing was titled “Revisiting the Need for Federal Data Privacy Legislation.” Although there appears to be growing consensus for the need for federal data privacy legislation, there remains no real consensus on the details of the legislation, including on federal preemption and a private right of action.</td>
<td>23 September 2020</td>
</tr>
<tr>
<td>California residents will vote on the California Privacy Rights Act, which, if passed, will impose increased privacy obligations on businesses that process California consumers’ personal information.</td>
<td>On 3 November 2020, California residents will vote on the California Privacy Rights Act (&quot;CPRA&quot;). If approved, the CPRA will become operative on 1 January 2023, and with the exception of the right of access, shall only apply to personal information collected by a business on or after 1 January 2022. The CPRA would replace the California Consumer Privacy Act and would impose additional requirements on companies to protect California consumers’ personal information from unauthorised or illegal access, destruction, use, modification or disclosure. The CPRA also contemplates the establishment of a new data protection agency, the California Privacy Protection Agency, which will have full administrative power, authority and jurisdiction to implement and enforce the CPRA. The California Privacy Protection Agency is expected to issue regulations that will require businesses to perform cybersecurity risk assessments and annual audits.</td>
<td>3 November 2020</td>
<td>California Privacy Rights Act</td>
</tr>
<tr>
<td>Businesses have at least another year to expand their privacy programmes to cover B2B and employee information.</td>
<td>The California Consumer Privacy Act (&quot;CCPA&quot;) B2B and employee data exemptions have been extended by one year. On 29 September 2020, Bill AB 1281 was signed into law extending the partial exemptions available for persons engaging in business transactions in their professional capacity as consumers, employees and job applicants until 1 January 2022 - if the Bill Passed: 3 November 2020</td>
<td>3 November 2020</td>
<td>Bill AB 1281</td>
</tr>
</tbody>
</table>
## United States

### Summary

California Consumer Privacy Rights Act ("CPRA") is not signed into law. If the CPRA is signed into law, businesses will have until 1 January 2023 to expand their privacy programs to cover B2B and employee information.

**B2B exemption:** Information handled in the context of B2B dealings, such as contact information of business representatives is exempt from certain provisions of the CCPA. An opt-out notice must be provided if B2B information is being "sold," but the requirement to provide B2B contacts a notice prior to the collection of their personal information or to provide them other consumer rights under the CCPA, such as the right to know and the right to delete has been waived until at least January 2022.

**Employee exemption:** Employee information, including information about job applicants, is also exempt from certain provisions of the CCPA. While businesses are required to provide a notice before collecting any personal information about employees or job applicants, there is no requirement to provide the right to know, the right to delete or the right to opt-out until at least January 2022.

If the CPRA is signed into law then AB 1281 will never go into effect but the CPRA will uphold the B2B and Employee Exemptions until 1 January 2023.

<table>
<thead>
<tr>
<th>Development</th>
<th>Summary</th>
<th>Date</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>California Consumer Privacy Rights Act (&quot;CPRA&quot;) is not signed into law. If the CPRA is signed into law, businesses will have until 1 January 2023 to expand their privacy programs to cover B2B and employee information. <strong>B2B exemption:</strong> Information handled in the context of B2B dealings, such as contact information of business representatives is exempt from certain provisions of the CCPA. An opt-out notice must be provided if B2B information is being &quot;sold,&quot; but the requirement to provide B2B contacts a notice prior to the collection of their personal information or to provide them other consumer rights under the CCPA, such as the right to know and the right to delete has been waived until at least January 2022. <strong>Employee exemption:</strong> Employee information, including information about job applicants, is also exempt from certain provisions of the CCPA. While businesses are required to provide a notice before collecting any personal information about employees or job applicants, there is no requirement to provide the right to know, the right to delete or the right to opt-out until at least January 2022. If the CPRA is signed into law then AB 1281 will never go into effect but the CPRA will uphold the B2B and Employee Exemptions until 1 January 2023.</td>
<td>January 2023</td>
<td>exemptions: 1 January 2022</td>
</tr>
</tbody>
</table>
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

@ESPrivacyLaw

**Editorial team**

**John Inglese**  
Senior Associate  
T: +44 20 7919 0955  
johninglese@eversheds-sutherland.com

**Lucy Clarkson**  
Apprentice Solicitor  
T: +44 113 200 4536  
lucyclarkson@eversheds-sutherland.com

**Joan Cuevas**  
Legal Technologist  
T: +44 20 7919 0665  
joancuevas@eversheds-sutherland.com

**Rosie Wallace**  
Apprentice Solicitor  
T: +44 20 7919 4942  
rosiewallace@eversheds-sutherland.com

**Thomas Elliott**  
Project Co-ordinator  
T: +44 1223 44 3675  
thomaselliott@eversheds-sutherland.com

**eversheds-sutherland.com**
© Eversheds Sutherland 2020. 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.
CAM_18_7125636\7