Bird & Bird

UK & EU Data Protection Bulletin: February 2021

Welcome to your monthly newsletter from Bird & Bird's UK Data Protection team

In this month's newsletter, we bring you the following updates:

United Kingdom

ICO

UK Cases

UK Law

EU and Council of Europe

EDPB

CJEU Cases

Other EU news

UK Enforcement

ICO Enforcement

United Kingdom

Information Commissioner's Office (ICO)

Date	Description
17 December 2020	On 17th December, the ICO submitted its Data Sharing Code of Practice, which was prepared under section 121 of the Data Protection Act 2018 ("DPA 2018"), to the Secretary of State which will lay the code before Parliament for its approval as soon as reasonably practicable. Once the Code has been laid, it will remain before Parliament for 40 sitting days. If there are no objections, it will come into force 21 days after that. The Code addresses many aspects of the DPA 2018 including transparency, lawful bases for using personal data, accountability principle, security and documenting the record of processing activities where the data sharing is between two or more controllers. Sharing data with processors is not covered by the Code. It aims to be a practical guide for organisations about how to share personal data in a compliant way and includes data sharing request form templates and checklists. In particular, it: • recommends that controllers carry out a data protection impact assessment particularly if the sharing involves a major project that involves disclosing personal data, or any plans for routine data sharing, even if there is no specific indicator of likely high risk; • requires the controllers to demonstrate a compelling reason when the data sharing involves children's personal data; • requires determining a lawful basis for sharing the personal data; • recommends putting a data sharing agreement in place; and • requires putting policies and procedures in the data sharing agreement to enable data subjects to exercise their rights. In particular, given data subjects can contact any controller involved in the sharing, the agreements should make clear that one staff member (generally a DPO in the case of personal data) or organisation takes overall responsibility for ensuring that the individual can easily gain access to all their personal data that has been shared. The Code also includes sections on data sharing by a competent authority for specific law enforcement purposes (as covered by Part 3 of the DPA 2018) as well as sections on sharing data for due diligence purposes, in databases and lists and in urgent situations. The Code also gives practical guidance on when and how to document the decision making involved behind data sharing. Alongside the Code, the ICO has launched a data sharing information hub where organisations can find more targeted support and resources.

UK Cases

Date	Cases
15 January 2021	Soriano v Forensic News LLC & Ors [2021] EWHC 56 (QB) The English High Court has accepted new arguments regarding the limits of the GDPR's territorial reach, in a case concerning online articles written about a UK resident. Noting that each of the defendants was a US resident, and not "established" in the UK for GDPR purposes (some UK-directed online activity being insufficient to qualify for those purposes), the High Court judge held that their publication of these articles could not be caught by GDPR Article 3(1) - the GDPR's "establishment" test. The judge focused instead on the GDPR's alternative territoriality tests: data processing is caught by the GDPR when it is related to the offer of goods or services to the data subject (Article 3(2)(a)), or to the monitoring of their behaviour (Article 3(2)(b)). The judge remarked that: 1) Although one of the sites offered to ship merchandise to the UK (and this may have happened on one occasion), this fact (alone) did not qualify as it "targeting" the UK with goods or services. Other EDPB "targeting" factors were not satisfied here. 2) A data controller may be subject to the GDPR in respect of some of its processing activities and not others. Here, the offer or goods or services was not "related to" the journalism. 3) Regarding the "behavioural monitoring limb", it was wrong for the claimants to point to the defendants' use of cookies on their websites (to personalise ads). This was unrelated to the impugned journalistic activities. To complain about the journalism, the journalism itself would need to amount to behavioural monitoring (something which the judge did not express a view on). The judge therefore struck out the GDPR claims, concluding there was no arguable case on that front. The case also offers readers an interesting discussion of related claims, including malicious falsehood, misuse of private Information, harassment and defamation.
19 January 2021	**R (on the application of M) v Chief Constable of Sussex & Brighton & Hove Business Crime Reduction Partnership [2021] EWCA Civ 42** This recent Court of Appeal decision looks at data sharing in the context of law enforcement purposes (under Part 3 of the DPA 2018 rather than under the GDPR) and involves M, a vulnerable teenager with previous criminal convictions who had been assessed as being at risk of child sexual exploitation, the police and a local crime reduction partnership (CRP) made up of more than 500 local businesses, retailers, bars and nightclubs. The police would often share data relating to individuals with the CRP under various information sharing agreements for law enforcement purposes so that the CRP could inform its management committee of issues concerning particular individuals, in order to take a decision

Date	Cases
	as to whether they should be excluded from entering certain commercial premises. The police would not share data with individual members of the CRP and the CRP would decide how to share the data with its members according to its own data sharing policy. In this case, the police shared information about M's name, date of birth, photograph and bail conditions with the CRP together with details of how she was linked to a police operation directed at vulnerable young women who were allegedly involved in anti-social/criminal behaviour in the local area. As a result of this information, the CRP made an exclusion order in relation to M. M then applied for judicial review of the lawfulness of the police's safeguards for disclosing sensitive data to the CRP under the information sharing agreement. Amongst other things, in determining whether the information sharing agreement was compatible with Part 3 of the DPA, consideration was given to: i) whether, to the extent that *sensitive* personal data was or might be shared with the BCRP, the information sharing agreement met the requirements for an "appropriate policy document" under section 42(2) DPA 2018 - the Court held that it did; and ii) whether the system of "technical and organisational measures" implemented by the police met the general requirements of "appropriateness" under Part 3. The general requirements apply to all personal data which is processed for law enforcement purposes, not just sensitive personal data; but the nature of the data would obviously be relevant when deciding whether the system afforded appropriate safeguards - the Court held that it did. Some other interesting points to note from this judgment include: (i) the fact whilst the GDPR specifically recognises the position of children and their vulnerability to the misuse of data, there is no equivalent provision in Part 3 of the DPA 2018 (which implements the Law Enforcement Directive). Lady Justice Andrews also acknowledged the fact that whilst the GDPR and Part 3 of the DPA both had 6 data protection principles, they were couched in slightly different terms and M's complaints related to the 1st and 6th principle; (ii) the CRP was not a "competent authority" for the purposes of Part 3 of the DPA 2018, so any onward disclosure by the CRP to its members would be was governed by the GDPR and not Part 3 of the DPA 2018 and the CRP would be acting as a controller in this regard (and not a processor on behalf of the police); (iii) the fact that whilst the High Court had held that information describing M as at risk of child sexual exploitation was "sensitive processing" (or in GDPR terms, special category data), the Court of Appeal concluded that such information was not as it was not data concerning M's sex life: "*....the natural understanding of that expression is that it relates to someone's own sexual behaviour, preferences, and lifestyle choices in that area, not to the fact that they are or have been at risk of being sexually abused or exploited by others. it is also difficult to envisage why data about the existence of that type of risk would be regarded as deserving of special protection and requiring specific justification which might act as a fetter on its dissemination*." (para 132). For a copy of the case see here.

UK Law

Date	Cases
1 January 2021	**Data Protection Act 2018 and UK GDPR amended by Data Protection, Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2020** As a result of the UK exiting the transition period of the UK-EU Withdrawal Agreement, and the marking of 'IP Completion Day', the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended by the 2020 Regulations we reported on in November) came into force. With the commencement of these Regulations, the UK GDPR has come into effect. The best reference for the UK GDPR remains the UK Government's Keeling Schedule, which has been updated to reflect the latest changes. Similarly, the Data Protection Act 2018 has gained a new Schedule 21, which includes transitional measures on topics such as data transfers. Again, the Government's updated Keeling Schedule best demonstrates these amendments, which at the time of writing are not available on the Act's page on legislation.gov.uk. As highlighted in November, the most pressing change in the latest UK regulations is to those organisations reliant on EU-authorised BCRs, which are not recognised as valid for UK transfers to third countries unless subsequently approved by the Commissioner.

EU and Council of Europe

EDPB

Date	Description
15 December 2020	**Guidelines 10/2020 on restrictions under Article 23 GDPR (currently under public consultation)** In December, the EDPB issued draft guidelines for consultation which aim to provide guidance as to the application of the Article 23 restrictions to data subject rights. Considering that the term ‘’restrictions” is not defined in the GDPR, the guidelines include a definition of ‘’restrictions” and provide a thorough analysis of the criteria to apply restrictions, the assessments that need to be observed, how data subjects can exercise their rights once the restriction is lifted and the consequences for infringements of Article 23. The guidelines analyse the grounds for restricting data subject rights (including national security and public defence, objectives of the general public interest, and the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions), analyse how the legislative measures laying out the restrictions should meet the foreseeability requirement (such as the need for specifying in the legislation the categories of personal data involved in restrictions of data subject rights). The EDPB mentions that restrictions which are extensive and intrusive cannot be justified to the extent that they void the fundamental right to the protection of personal data. The guidelines provide for an explanation on the "necessity and proportionality" test that such restrictions need to pass. Moreover, the guidelines outline the European Commission’s monitoring powers on whether national legislation complies with Article 23 GDPR requirements, alongside setting out the enforcement powers for national supervisory authorities in cases where, the data controller infringes such measures. The consultation runs until 12 February 2021.
14 January 2021	**EDPB and EDPS issue joint opinions on the Standard Contractual Clauses for data transfers and for data processors** The EDPB and EDPS recently issued their joint opinions on the recent draft Standard Contractual Clauses put forward by the Commission in November 2020 to address data transfers to third countries and Article 28 provisions between controllers and processors. **Draft Decision and Data Transfer Clauses** Overall, the EDPB and EDPS seem satisfied that the Draft Decision and Data Transfer Clauses bring a reinforced level of protection for data subjects and they welcome the specific provisions intending to address some of the main issues identified in the Schrems II ruling. However, the EDPB and EDPS call on the Commission to clarify that there may still be situations where, despite the new Clauses, ad hoc supplementary measures will remain necessary to be implemented in order to ensure that the data subjects are afforded a level of protection essentially equivalent to that guaranteed in the EU. As such, the Clauses will have to be used along with the EDPB Recommendations on supplementary measures.

	Nevertheless, the EDPB and EDPS are of the view that several provisions could be improved or clarified, such as whether the modules can be included in one set of the Clauses to address different scenarios or if several sets still need to be signed; the scope of the Data Transfer Clauses and their interplay with the Draft Data Processor Clauses; certain third party beneficiary rights; whether the Clauses can be used in joint controllership scenarios where one of the joint controllers is outside the EU and not subject to GDPR; certain obligations regarding onward transfers; aspects of the assessment of third country laws regarding access to public data by public authorities; and the notification to the Supervisory Authority. The EDPB and EDPS also understand that the Draft Decision does not cover (i) transfers to a data importer not in the EEA but subject to the GDPR for a given processing under Article 3(2) GDPR and (ii) transfers to international organisations. However they recommend that the Commission clarifies that these provisions are only intended to address the issue of scope of the Draft Decision and the draft Clauses and not the scope of the notion of transfers (otherwise this could be interpreted so that if a controller/processor is directly subject to Article 3(2), they don't have to comply with the data transfer requirements). Additionally, the EDPB and EDPS suggest that the Annexes to the Clauses clarify as much as possible the roles and responsibilities of each of the parties with regard to each processing activity as well as providing some technical drafting suggestions. **Draft Data Processor Clauses** In general, the EDPB and EDPS welcome the adoption of such Clauses as a strong accountability tool but again have suggestions for improvements and have requested clarifications for instance on scope, obligations of the parties and data subject rights, Again the importance of the Annexes is also emphasised whereby they must with absolute clarity delimit the roles and responsibilities of each of the parties in each relationship and with regard to each processing activity. For details of the Opinions, see here: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en
18 January	**New guidelines on examples regarding data breach notification** On 18 January, the EDPB adopted guidelines to complement the WP 29 guidance on data breach notification by providing practical examples of data breaches. They aim to help data controllers in deciding how to handle data breaches and what factors to consider during risk assessment. The guidelines contain an inventory of data breach notification cases deemed most common by the national supervisory authorities (SAs), such as ransomware attacks; data exfiltration attacks; and lost or stolen devices and paper documents. The guidelines present the most typical good or bad practices, advice on how risks should be identified and assessed, highlight the factors that should be given particular consideration, as well as inform in which cases the controller should notify the SA and/or notify the data subjects. The guidelines will be submitted for public consultation for a period of six weeks.

CJEU

Date	Description
11 November 2020	**Orange România SA v Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) C-61/19** In November 2020, the CJEU issued its decision on the Orange Romania case (C-61/19) which examines the concept of consent. Earlier this year we had looked into Advocate General's opinion on the same case. The referral was made in the context of a dispute between Orange Romania and the Romanian Data Protection Authority, the ANSPDCP, in which Orange Romania challenged the ANSPDCP's decision to issue a fine against it for storing copies of customers' identity documents without demonstrating that those customers had provided valid consent and the ANSDPCP's order to Orange Romania to destroy the relevant data. When signing up for Orange Romania's telecommunication services, Orange Romania's practice was to take a copy of customers' identity documents, which it would then store as an attachment to the signed customer contract. The contract included a data protection clause, among other clauses, which affirmed that the customer had been informed of, and had consented to, the collection and storage of those copies for identification purposes. This clause was accompanied by a tick box which had been checked for some contracts, while for others it remained blank. Orange had stated that this box was checked by its sales agents, who informed the customer of the relevant processing and obtained their oral consent prior to the conclusion of the contract. Despite the existence of this clause, Orange let customers to sign up for the service even when they refused to consent; however, in such cases, Orange requested that the customer set out their refusal in a specific form. The Court examined Orange Romania's practices both under the Data Protection Directive and the GDPR, as it considered both to be relevant in the case in question. In interpreting the legal provisions relating to consent, the CJEU concluded that it is for the data controller to demonstrate that the data subject has, by active behaviour, given their consent and that they have received beforehand sufficient information, in an intelligible and easily accessible form, using clear and plain language, allowing that person to understand the consequences of the consent, so that they can provide it with full knowledge of the facts. On this basis, the Court identified several points in Orange's practices which could fall short of the required standard of consent: • the mere fact that the relevant box was ticked was not such as to establish a positive indication of customers' consent (the box was ticked by Orange's sales agents and not the customers); also, the fact that those customers signed the contract which contained the ticked box would not on its own prove such consent, to the extent there are no indications confirming that those customers had actually read and digested the relevant data protection clause; • the informed nature of consent would be called into question where the terms of the contract are capable of misleading the data subjects as to the possibility of concluding the contract even if they refused to consent; • the fact that customers had to complete an additional form to indicate their refusal to consent could unduly affect the customers' freedom to object to the processing of their ID copies: the data controller cannot require individuals actively to express their refusal. The full text of the decision is available here.

Other EU News

Date	Description
10 December 2020	**Cookies: CNIL issues fines to Google and Amazon for a total of €135 million** On 10th December, the French Data Protection Authority (i.e. the CNIL) released details of two financial penalties issued against Google (€100 million in total – €60 million for Google LLC and €40 million for Google Ireland Ltd) and Amazon Europe Core (€35 million). These sanctions have been issued on the basis of rules that were in place in the CNIL's 2013 cookie guidance (rather than the revised guidelines issued in October 2020 and to which a 6 month grace period applies. The CNIL also confirmed that it is materially competent to issue sanctions for breach of the so called "cookie rules" coming from the ePrivacy Directive (and Article 82 of the French Data Protection Act) for users living in France. The GDPR "one stop shop" mechanism does not directly apply in this case as rules around cookies and similar trackers fall under the ePrivacy directive. The CNIL also indicated to be territorially competent under Article 3 of the French Data Protection Act as the use of cookies by Amazon and Google was carried out "in the context of the activities" of the companies' establishments in France (i.e. Google France is an establishment of Google LLC and Google Ireland Ltd; and Amazon France is an establishment of Amazon Europe Core). Both sanctions are focused on very similar points: 1. Cookies being placed without prior consent: Advertising cookies were placed as soon as a user landed on the companies' websites before any action from the user (even "continued browsing" which would have been valid under the 2013 guidelines). Therefore, the user's consent was not given prior to cookies being placed. The CNIL states that this practice is by nature "incompatible with prior consent". Note that in both cases (Amazon and Google), the companies claimed to have addressed this point via updated solutions rolled out in September. 2. Lack of transparency and attempts to remediate The mechanisms deployed by Google and Amazon at the time of the CNIL's investigations were structured as follows: • Google: An information banner displayed at the bottom of the page entitled "Privacy reminder from Google", in front of which were two buttons: "Remind me later" and "Access now". • Amazon: the following information banner was displayed: "By using this website, you accept our use of cookies allowing to offer and improve our services. Read More". The CNIL also noted that the banner was not displayed in cases where users had previously clicked on an Amazon ad on another website. The CNIL found that both banners did not contain sufficient information to inform users about (i) the purposes of the trackers being placed in particular personalised advertising and (ii) how to reject cookies.

Date	Description
	The CNIL emphasised the need to give clear information about cookie purposes in the first layer of the banner displayed. The CNIL specified that the wording "to offer and improve our services" in Amazon's case was not clear enough to inform users that trackers were placed for personalised advertising purposes. The CNIL also dismissed Google's argument that such information could be displayed in a second layer of information. Google rolled out an update in September to try to address this question. Google now displays a pop up with additional wording and two options "more information" and "accept". The CNIL also concluded that this update wasn't compliant despite recognising that this was a step in the right direction in terms of information. It indicates that the information displayed wasn't clear, specific enough and/or complete and that the words "options" or "more information" aren't sufficiently explicit to allow users to understand that they have the right to reject trackers. In its press release published alongside the decision, the CNIL also indicates to have noticed Amazon's recent update to try to address this question. However, similarly to Google, it concludes that it still doesn't allow users to understand that trackers are mainly placed to display personalised ads and that they can be refused. **Key takeaways:** • The GDPR one stop shop mechanism doesn't apply to enforcement actions taken on the basis of the ePrivacy regime (Article 82 of the French Data Protection Act). • As previously announced, the CNIL is actively enforcing cookie obligations that haven't been modified by its updated Cookie guidance (published in October 2020) – where websites and/or apps are not compliant with the previous rules (based on the CNIL cookie guidance from 2013), remediation actions should not wait the end of the grace period for the new guidance (March 2021). • Only place or access cookies or similar trackers (subject to consent requirements) once users have consented. Trackers must not be placed as soon as the user lands on the website. • Transparency is key - users must be clearly informed of the purposes for which trackers are placed and of their right to withdraw consent/change their preferences • Mechanisms allowing users to change their preferences must be easily accessible.
15 December 2020	**Conclusion of investigation into Twitter** On 15th December, the Irish Data Protection Commission (**DPC**) announced a conclusion to a GDPR investigation it conducted into Twitter International Company. The DPC's investigation commenced in January 2019, following receipt of a breach notification from Twitter and the DPC has found that Twitter infringed Article 33(1) and 33(5) of the GDPR in terms of a failure to notify the breach on time to the DPC and a failure to adequately document the breach. The DPC has imposed an administrative fine of €450,000 on Twitter for these breaches. The level of penalty was confirmed by the EDPB after a dispute arose between the DPC and other data protection authorities across Europe over the DPC's enforcement in the case. It is the first time the EDPB has had to step in to resolve such a dispute between data protection authorities using the Article 65 process under GDPR and its decision is available here.

UK Enforcement

UK ICO Enforcement

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
13 November	Ticketmaster UK Limited	Monetary penalty of £1.25 million	The Information Commissioner's Office (ICO) has fined Ticketmaster UK Limited £1.25million for failing to keep its customers' personal data secure. The ICO found that the company failed to put appropriate security measures in place to prevent a cyber-attack on a chat-bot installed on its online payment page. The data breach, which included names, payment card numbers, expiry dates and CVV numbers, potentially affected 9.4million of Ticketmaster's customers across Europe including 1.5million in the UK. Investigators found that, as a result of the breach, 60,000 payment cards belonging to Barclays Bank customers had been subjected to known fraud. Another 6,000 cards were replaced by Monzo Bank after it suspected fraudulent use. The ICO found that Ticketmaster failed to: • Assess the risks of using a chat-bot on its payment page • Identify and implement appropriate security measures to negate the risks • Identify the source of suggested fraudulent activity in a timely manner
26 November	AMS Marketing Limited	Marketing Company Director gets banned by Insolvency Service for 6 years	Director, Elia Bols, of AMS Marketing Limited (a telephone marketing company), who made over 75,500 unsolicited marketing calls, has been banned by the Insolvency Service for six years. AMS Marketing Limited did not use the TPS list before making such calls to remove the numbers of individuals who had elected not to receive unsolicited contact. The Telephone Preference Service (TPS) received 71 complaints between October 2016 and October 2017 about AMS Marketing's unsolicited calls. A further 32 complaints were received by the Information Commissioners Office (ICO), who informed Elia Bols that a fine of £100,000 would be issued. On 28 October 2020, the Secretary of State accepted a disqualification undertaking from Elia Bols after he did not dispute that he had caused his company to breach Regulation 21 of the Privacy and Electronic Communications Regulations in making the marketing calls.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
4 December	OSL Financial Consultancy Limited (OSL)	Monetary penalty of £50,000	The Information Commissioner's Office (ICO) has fined OSL Financial Consultancy Limited (OSL) £50,000 for illegally sending 174,342 nuisance marketing texts. This mortgage and loans broker, trading as MortgageKey, came to the attention of the ICO as part of its probe into companies seeking to take advantage of the Covid-19 pandemic with nuisance marketing. Between March and June 2020, the ICO identified a number of complaints about OSL that had been sent to the 7726 spam text reporting service. The complaints related to nuisance text messages received by the public about a drop in Buy to Let mortgage interest rates. The ICO investigation found 54,205 nuisance texts were sent during the pandemic, with 120,137 nuisance texts sent in the months earlier. Throughout the ICO's enquiries, OSL relied on the previous consent it said it had obtained from its customers. The ICO's investigation found OSL had gathered personal data from people who had contacted them via their website to obtain a quote and then used the data for marketing purposes. People were not offered the option to opt in or out of marketing, and the ICO concluded that valid consent had not been obtained. This is against electronic marketing law.
9 December	Pension House Exchange (PHE)	Monetary penalty of £45,000	Pension House Exchange (PHE) has been fined £45,000 for making more than 39,000 nuisance calls to people about their pensions in breach of new laws linked to pensions cold calling. Under the law, companies can only phone and talk to people about their occupational or personal pensions if: - the caller is authorised by the Financial Conduct Authority (FCA), or is the trustee or manager of an occupational or personal pension scheme, and - the recipient of the call consents to calls, or has an existing relationship with the caller. After raiding PHE's offices as part of an investigation, the ICO found that PHE staff connected with people on LinkedIn and harvested their contact details to target them with direct marketing calls relating to pensions schemes.

Date	Entity	Enforcement notice, undertaking, monetary penalty, or prosecution	Description of Breach
16 December	Pownall Marketing Limited	Proceedings for monetary retrieval from company that was fined by ICO	The ICO's Financial Recovery Unit (FRU) is starting proceedings to retrieve £250,000 from defunct company, Pownall Marketing Limited (PML). The company was recently fined by the ICO for making over 350,000 nuisance calls. PML came to the ICO's attention when it began receiving complaints about nuisance marketing calls, relating to claims management services, made by the company. The ICO's investigation found that 365,369 calls had been made between 1 January and 28 May 2019 to people who had not consented to receive them. The FRU has blocked PML's application to strike itself off the Companies House register three times, ensuring the ICO can continue regulatory action. If the company fails to pay the penalty then the FRU will take appropriate action to recover the debt, which may involve petitioning for the winding up of the company and exercising the ICO's full rights as a creditor in any insolvency.
08 January	Kim Doyle	Imprisonment sentence as a result of Computer Misuse Act prosecution brought by ICO	A motor industry employee has been sentenced to eight months' imprisonment, suspended for two years, in a prosecution brought by ICO. An ICO investigation found that Doyle unlawfully transferred the data she obtained to William Shaw, the director of an accident claims management firm, TMS (Stratosphere), trading as LIS Claims. There is evidence this data was used to make nuisance calls. Doyle, who worked for the RAC, pleaded guilty to charges of conspiracy to secure unauthorised access to computer data, and to selling unlawfully obtained personal data to an accident claims management firm without authorisation. The court heard that Doyle compiled lists of road traffic accident data including partial names, mobile phone numbers and registration numbers despite having no permission from her employers. Another individual, Shaw, was also sentenced to eight months' imprisonment, suspended for two years after pleading guilty to conspiracy to secure unauthorised access to computer data in connection with the same event. Doyle and Shaw were also each ordered to carry out 100 hours unpaid work and contribute £1,000 costs. A Confiscation Order, under the Proceeds of Crimes Act, to recover benefit obtained as a result of the offending has been given by the Court in which Doyle must pay a benefit figure of £25,000 and Shaw must pay a benefit figure of £15,000. Both Doyle and Shaw will face three months' imprisonment if the benefit figures are not paid within three months.

Other recent articles

What does the Brexit Agreement say about Data Protection?

The European Commission's proposed Data Governance Act

HR Essentials

Governments around the world are now racing to approve and roll out various vaccines in an attempt to gain control over the spread of the virus. There are pressing employment and data protection issues around this in relation to the workplace and more broadly, including around requesting and handling information regarding employee vaccine status, mandating vaccination for access to workplaces, and more. To address this, we have updated our COVID-19 chart which has been developed to help employers prioritise and understand these questions through a traffic light system, as well as detailed responses to some pressing questions.

For any organisation, equality, diversity and inclusivity are key cornerstones to building a strong, engaged and open workforce. Often, the first step for many employers is to collect data from their employees and other members of staff on a range of matters in this area. Bird & Bird has produced guidance to help you.