Bird & Bird

European Data Protection Bulletin

March 2023

Welcome to our regular European Data Protection Bulletin

In this edition, we bring you the following updates:

EDPB

Date	Description
18 January	**EDPB adopted a report on the work undertaken by the Cookie Banner Task Force** **Cookie Banner Taskforce** On the 18th January the EDPB's Cookie Banner taskforce released its report. This taskforce was set up in response to the ongoing project by the campaign group, NOYB, which has written to a variety of companies to allege their cookie banners breach either the ePrivacy Directive, or the GDPR. The taskforce has since considered each of the main types of "infringement" that NOYB has claimed, with the report explaining their views on the minimum threshold for each requirement. ***Taskforce Conclusions*** **1. "Reject All" on the First Layer** This topic was the only one where a split verdict was noted. The "vast majority" of supervisory authorities noted they consider a banner which does not have a "Reject" (or equivalent) button on the first layer to be in breach of the ePrivacy Directive, however the report notes that "[a] few authorities" disagreed. The latter group argued that such an option is not explicitly required by the Directive. It is worth noting that ePrivacy requirements can often be enforced based on the local laws of the website user. As such it is likely to be preferable to adopt the stricter approach of requiring a button for all EEA users. **2. Pre-Ticked Boxes in the Second Layer** The taskforce went on to consider the impact of pre-ticking boxes for certain types of cookies in the second layer, where the user is given the choice of accepting or rejecting specific types of cookies. Here the taskforce had no problem confirming that pre-ticked boxes cannot lead to valid consent, referring in particular to the explicit statement of this in recital 32 of the Directive. **3. Deceptive Link Design** This refers to cases where there is an option to refuse to provide consent for cookies, however this option is provided in a way which is not clear to the user. The taskforce specifically called out having this option embedded in a paragraph of text or elsewhere on the page, rather than in the banner itself,

Date	Description

as examples which would normally invalidate consent (unless there was "sufficient visual support to draw an average user's attention" to this alternate option).

Beyond these two examples, the taskforce chose to reiterate that valid consent for cookies requires the user to understand what they are consenting to, how to provide consent, and for consent to be freely given. Furthermore, the taskforce stressed that the user must not be given the impression that they have to consent to (non-necessary) cookies to access the website, nor may the user be pushed to give consent.

4. Deceptive Button Colours and/or Contrast

Under this heading, the taskforce limited any specific criticism to the point where the alternative action (other than giving consent) was offered in a way that the text is unreadable to virtually any user. Beyond this the taskforce refused to give any more comments on requirements for colour and contrast, instead stressing that this needs to be assessed on a case-by-case basis. They note the test to be applied is whether the contrast and colours used are "obviously misleading for the users" and whether they result in an unintended (and therefore invalid) consent.

5. Legitimate Interest Claimed in Cookie Banner

The taskforce noted that information contained in a cookie banner can cover both processing in the context of placement and retrieval of information in a cookie, and processing in the context of further use of that information (e.g. in creating a profile of the user). Each of these operations require a lawful basis, and the lawfulness of a website claiming "legitimate interests" as the legal basis of processing in a cookie banner depends on which of these operations the claim relates to.

The taskforce reiterated that "legitimate interests" is not a valid basis for storing cookies on a user's device or reading cookies. The taskforce recognised that legitimate interests could apply to processing of data derived from cookies (which is solely regulated by the GDPR), but care must be taken to ensure the user is not confused by this. In particular, the user should not be allowed to think they need to refuse twice to prevent their personal data being processed. The taskforce also noted that if the cookies are not placed and retrieved in compliance with the ePrivacy directive, then further processing of information derived from those cookies can never be compliant with GDPR.

6. Inaccurate Classification of "Essential" Cookies

The taskforce recognised that classification is difficult, particularly considering that the use of cookies could change regularly in the development of a website. The taskforce discussed the existence of tools to establish the list of a cookies as well as the responsibility of website owners to maintain a list and to provide them to supervisory authorities on request and to be able to demonstrate why certain cookies are essential.

The taskforce provided little further detail on this topic, only noting that tools existed to help this task but that these tools did not provide details of the nature of the cookies and referring back to previous guidance on the topic.

7. No Option to Withdraw Consent

Date	Description
	Finally, the taskforce considered cases where the website operator does not provide an option to withdraw consent which is as easy as granting consent. In particular, the taskforce addresses NOYB's suggestion that a persistent "floating" button is needed to satisfy this, with the taskforce noting that this is not required (although such an option would be compliant). Instead, website owners only need to place an "easily accessible" solution, with the ease of this solution to be assessed on a case-by-case basis. In particular a "link placed [i]n a visible and standardized place" is specifically mentioned as a valid alternative. ***Comment*** This further guidance mostly restates already established guidance, but it is useful to note that there is a degree of pushback on NOYB's more extreme stances. This is particularly visible on the topic of deceptive button contrast and colours, and when discussing the need for an easy method of withdrawing consent. Here the EDPB taskforce firstly only ruled out the most extreme abuse where the text was made unreadable and made it clear that there is no strict universal requirement around colour and contrast, and secondly stressed that NOYB's preferred choice to withdraw consent (in the form of a floating button) was absolutely not a requirement. With more waves of complaints planned by NOYB, this will provide a useful guide as to where compliance with NOYB's demands is required, and where more flexibility may be available.
5 December 2022	The European Data Protection Board issued binding decisions under the Art.65 dispute resolution process to the Irish Data Protection Commission. The DPC adopted associated decisions on 31 December 2022 and 12 January 2023. The Facebook and Instagram decisions concluded that Facebook and Instagram were processing personal data for certain behavioural advertising activities without a lawful basis and that such processing was unfair; in addition, there were failings of transparency in relation to privacy notices. Fines of €210M and €180 M were imposed respectively. The WhatsApp decision found that WhatsApp was processing personal data for service improvement and safety and security purposes without a lawful basis and unfairly; a fine of €5.5M was imposed. The decisions are analysed in detail here: Meta – DPC & EDPB Decisions on lawful basis of processing and transparency
14th February 2023	**EDPB adopts work programme for 2023/2024** This is a continuation of existing activities (guidance; consistency and co-ordination; opinions to EU bodies). There is a list of planned guidance – many of the entries in this are carried forward from the previous period, where the EDPB has not been able to conclude the guidance in the time planned. For example, anonymisation, pseudonymisation, childrens data and scientific research are all mentioned (again) in the work programme.

Date	Description
	Guidelines are planned on: subject access; lead supervisory authority update; breach notification update; guidelines on technology to detect and report on CSAM; legitimate interest; children's data; medical and scientific research processing; social media use by public bodies; fines, mutual assistance, the right to be heard under art.60, anonymisation, pseudonymisation, blockchain, telemetry and diagnostic data and the interplay between the AI Act and GDPR. The EDPB also plans templates for data subject complaints.
	EDPB adopts guidelines on deceptive design patterns, certification as a tool for transfers and the interplay between Art.3 and Chapter V For our webinar on Deceptive design patterns see here On the guidance on the interplay between Art.3 and Chapter V it's worth noting that the EDPB has added in new content addressing the appointment of processors within the EU, but which could be subject to laws with extra-territorial effect, obliging them to disclose personal data to public authorities in third countries. Here, EDPB says that art.28 requires that the controller must only use processors who will meet the requirements of GDPR and that this entails an obligation on the controller to consider the reliability of processors that could be subject to these types of obligations.

CJEU

Date	Description
16 December	**AG limits the expansive interpretation of what constitutes personal data** The Advocate General's ("**AG**") opinion, published on 16.12.2022, considers whether an individual is entitled to learn which natural person has accessed that person's personal data. In other words: When a person in an organization views your personal data, is the identity of the person viewing your data actually your personal data? **Facts of the case** The data subject, J.M, worked in a Finnish bank and was also a customer of the bank. During 2014, employees of the bank accessed J.M's customer data. In May 2018, right after GDPR became applicable, J.M wanted the bank to reveal the identity of the employees who had accessed his data. He also wanted to know the purpose of the processing. According to the Article 15 (1) GDPR, *1.The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:* *(a) the purposes of the processing;* *(b) […];* *(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;* J.M. was unlucky as the bank refused the request and the Finnish DPA agreed with the bank in 2020. Before the Finnish DPA, J.M. argued that if data subjects did not have a right to obtain the identity of the persons who had accessed their personal data, data subjects would have no effective means of verifying the lawfulness of the processing. J.M. brought the case to the Finnish Administrative Court which asked the CJEU for a preliminary ruling.

Date	Description

The Administrative Court referred the following questions to the CJEU:

- In the event someone views a data subject's personal data, should log data generated by this activity (indicating specifics of the viewing) be considered as the personal data of the data subject whose data has been viewed, considering in particular the fact that it also contains data of a third person?
- If the log data does not constitute personal data of the person whose personal data has been viewed and the person subsequently does not have the right of access to the log data under GDPR 15(1), the following questions remain open:
- Does the right to know the purpose of the processing under GDPR 15(1)(a) give the data subject a right to get to know who the persons were who viewed the data subject's personal data?
- In this context, should the persons who viewed data subjects' data be considered as recipients of personal data as referred to in GDPR 15(1)(c) and would data subject therefore be entitled to obtain information of the recipients?
- Is it of relevance in the present case that the bank in question is performing a regulated activity or that J.M. was both an employee and a customer of the bank at the same time?
- Is the fact that J.M.'s data were processed before the entry into force of the GDPR relevant to the examination of the questions set out above?

Answers from the AG

The AG reduced the questions of J.M. to the core and focused on the question whether "*the identity of the employees who consulted J.M.'s data does not constitute his 'personal data'*".

The AG came to the conclusion that it was not J.M.'s data, but the bank's employees' data.

According to the AG, the access right under Article 15 had two dimensions: First, it gave data subjects the right to obtain *"confirmation as to whether or not personal data relating to him or her are being processed"*. This interest was satisfied here, as J.M. knew what personal data was processed by the bank. Secondly, Article 15 grants a right to access to *information*, not *personal data*, provided in the letters (a) to (h) of the GDPR Article 15 (1).

Could one argue than that the employees of the bank were "recipients" according to Article 15 (1)(c)? The AG analysed the term "recipient" and stated that

"the concept of recipient does not include employees of a legal person who, when using the latter's computer system, consult the personal data of a client on behalf of its administrative bodies. Where such employees act under the direct authority of the controller, they do not, on that basis alone, acquire the status of 'data recipients'."

In other words, those that act under the authority and within the instructions of an organization are not recipients, and their identity does not have to be provided. The AG also considered that employees of banks could be pressured if data subjects had the right to know who was working on their case.

The AG also confirmed that data subjects may exercise the procedural right of access under the GDPR even in case the processing has taken place before its applicability. In these cases, consideration to the laws which were in place during that time must naturally be considered. In this case however, the access

Date	Description
	request came when the GDPR was already applicable. Also, AG's viewed it irrelevant for the legal consideration that J'M was both an employee and a customer of the bank and that the bank carried out a regulated activity. **Reflections on the AG's opinion** The case can be seen as a continuation of CJEU cases where the interpretation and limits of personal data have been analysed. So far, the court has been consistently inclined to take a wide interpretation of what constitutes personal data, one might even say the widest possible interpretation. This is evidenced in its rulings in cases such as Lindqvist C-101/01, Breyer C-582/14, Novak C-434/16 and most recently Vyriausioji C-184/20. In these cases, the CJEU has viewed health data, IP address, examination scripts and sexual orientation related data in a rather expansive way. While most data protection practitioners would hope for some limitations on the definition of what constitutes personal data, we will have to wait for the final court decision. The well-balanced AG opinion gives some hope. For a copy of the AG's Opinion: see here
12 December	**TU and RE v Google LLC Case C-460/20 : impact of inaccuracy on erasure requests to search engines; and CJEU confirms the adage that a picture is worth a thousand words** **Factual background** TU and RE made de-listing requests to Google relating to three articles published about them, criticising the investment model of one of the companies they were involved with (as shareholder/directors/having general commercial power in a group of companies). One of the articles contained three images of TU in front of a luxury car, helicopter, and a plane. The article also contained an image of RE in a convertible car. The articles and images were searchable on Google, when entering TU and RE's names or certain company names. TU and RE made de-listing requests to Google on the basis that the articles contained inaccurate claims and defamatory opinions. They also made requests for the images to be removed from the thumbnails in the search results. Google refused to comply with the requests and argued that the claimants had not proven the inaccuracy of the information in the articlesA request for preliminary ruling was made to the CJEU by the German courts. **The judgment** On inaccuracy, the CJEU concluded that: • if a data subject submits a de-listing request, on the basis that the objected-to content is inaccurate, it is not necessary for the data subject to have proven inaccuracy by proceedings against the original publisher [77];

Date	Description
	• the data subject does, however, have to be able to demonstrate that at least some of the objected-to content is inaccurate; it is not sufficient for the data subject to show that a minor part of the content, by comparison to the content as a whole, is inaccurate; the evidence required is limited to what is reasonable – it would not be reasonable to require the individual to have obtained an interim decision against the publisher as this would effectively remove the right to erasure [68]; • if the data subject establishes this then, the search engine should de-list the original content [72]; • however, if the data subject cannot establish this, then there is no obligation on the search engine to undertake independent steps to evaluate the accuracy of the information [71]; also, if the inaccuracy only relates to a minor part of the content, there is no de-listing obligation [74]; • if the search engine does not de-list then there must be a right for the data subject to complaint to a supervisory authority, which would then have the obligation to determine the approach [75]; and • where it is brought to the attention of the search engine that there are pending proceedings relating to inaccuracy of content, then the search engine must include a warning to this effect when it displays results [76]. On inclusion of thumbnail images, the court concluded that: • a search engine has the same obligations in dealing with delisting requests involving images as it does with other de-listing requests [90]; • however, the intrusion on private life when images are returned in response to an image search is particularly acute [95], [100]; • accordingly, when a de-listing request is made in relation to images, the search engine must consider whether publication of the images per-se (as distinct from other information) is necessary for freedom of expression. The search engine must carry out a separate balancing test to the original publisher, as the publication of the images in the original article will usually have been done to illustrate particular textual points, whereas the return of images alone in response to a search request, will raise different issues [101]; • because pictures have a stronger impact on individuals, if a request for de-referencing of a web-page is rejected, a search engine may still have to de-reference images contained in that web-page; this must be considered separately [106]. For a full copy of the case see here
12 January	**C-154/21 (Österreichische Post): Information about the recipients or categories of recipient to whom the personal data have been or will be disclosed** In its decision from 12th January 2023, the CJEU ruled on certain aspects of the data subjects' right of access pursuant to Art. 15 GDPR. Art. 15 (1)(c) GDPR implies that where personal data have been or will be disclosed to recipients, the controller is obligated – upon request – to provide data subjects with the

Date	Description

actual identity of those recipients. Only where it is not (yet) possible to identify those recipients, controllers may indicate only the categories of recipients in question. That is also the case where the controller demonstrates that the request is manifestly unfounded or excessive.

FACTS OF THE CASE

On 15 January 2019, a data subject (DS) requested access to his personal data (PD) processed by the Österreichische Post AG (the Austrian postal service - PS). DS requested information from PS whether and which personal data concerning him were being stored or had previously been stored by PS, if his personal data had been disclosed to third parties and if so, information as to the identity of the recipients. However, PS provided merely generic answers to this request and referred to its online privacy policy.

Subsequently DS brought proceedings against PS in front of the Austrian courts, seeking an order that PS provides him with, amongst other things, the identity of the recipient(s) of the personal data disclosed. iIn the further course of the proceedings, PS disclosed that the personal data was processed for marketing purposes and forwarded to customers, including advertisers trading via email order, mailing list providers or political parties. The courts at first instance and on appeal dismissed DS's action on the ground that Art. 15(1)(c) GDPR, by referring to 'recipients or categories of recipient', gives the controller the option of informing the DS only of the categories of recipient, without having to identify by name the specific recipients to whom personal data are transferred.

DS brought an appeal on a point of law before the Austrian Supreme Court (OGH), the referring court. The OGH referred the following question to the CJEU for a preliminary ruling:

'Is Article 15(1)(c) of [the GDPR] to be interpreted as meaning that the right of access is limited to information concerning categories of recipient where specific recipients have not yet been determined in the case of planned disclosures, but that right must necessarily also cover recipients of those disclosures in cases where data [have] already been disclosed?'

RULING

Article 15(1)(c) of the GDPR "*must be interpreted as meaning that the data subject's right of access to the personal data concerning him or her, provided for by that provision, entails, where those data have been or will be disclosed to recipients, an obligation on the part of the controller to provide the data subject with the actual identity of those recipients, unless it is impossible to identify those recipients or the controller demonstrates that the data subject's requests for access are manifestly unfounded or excessive within the meaning of Article 12(5) of Regulation 2016/679, in which cases the controller may indicate to the data subject only the categories of recipient in question*".

CJEU'S CONSIDERATIONS

- **Art. 15 (1)(c) GDPR is unclear, but Rec. 63 indicates identity of recipient has to be disclosed**

Date	Description

Art. 15 (1)(c) GDPR does not clearly stipulate whether a data subject has the right to be informed of the specific identity of her/his PD's recipients. However according to Rec. 63 the data subject should have the right to know and obtain communication in particular with regard to the recipients of the personal data without restriction solely to categories of recipients.

- **Principle of transparency must be adhered to in order to respect right of access**
  Right of access demands that all processing of PD must comply with GDPR principles, in particular covering the principle of transparency. Accordingly, the data subject must receive information about how her/his PD is processed in easily accessible and understandable way.

- **Art. 15 GDPR is a data subject right**
  In comparison to Art. 13/14, Art. 15 GDPR lays down a right of access for the data subject, but not a pro-active obligation for the controller. Hence, it is up to the data subject to decide whether information of specific recipients or only categories of them are provided.

- **Right of access provides basis for other data subject rights**
  Right of access is necessary to enable the data subject to exercise other rights. To ensure the effectiveness of these rights, the data subject must therefore *"[…] have, in particular, the right to be informed of the identity of the specific recipients where his or her personal data have already been disclosed*". This is confirmed by Art. 19 GDPR, which provides that the controller has to communicate any rectification or erasure of PD or restriction of processing to each recipient to whom the PD has been disclosed. Also the controller has to inform the data subject about those recipients if requested by the data subject.

- **Art. 15 (1)(c) GDPR could be restricted in certain cases**
  CJEU emphasised, that the right to the protection of personal data is not an absolute right. That right must be considered in relation to its function in society and be balanced against other fundamental rights. In specific circumstances it may be acceptable for controllers not to provide specific recipients, but only categories of recipients:

  - If it is not possible to provide information about specific recipients (in particular where they are not known yet)
  - If the request is manifestly unfounded or excessive (controller needs to demonstrate this).

WHAT DOES THIS MEAN?

This decision provides clarification on a topic burdensome for controllers. The CJEU interprets Art. 15. (1)(c) GDPR in a way that controllers have to disclose the identity of the PD's recipients if requested by a data subject. It is fair to state that this ruling is in line with already existing expectations of the stricter courts and DPAs in EU jurisdictions (e.g. Germany). Ultimately this will result in additional administrative and legal work for controllers. It is noteworthy that the CJEU's exemptions to its strict interpretation of Art. 15 (1)(c) GDPR are not new. Already before this decision it has been clear that a controller cannot name a recipient if it is unknown. The exemption applicable if the controller can prove that an access request is manifestly unfounded or excessive is also well known. The CJEU mentions that data subject rights have to be balanced against other fundamental rights but does not elaborate on this aspect further. **For more details of the case, see here**

Date	Description
9th February 2023	**X-FAB Dresden GmbH & Co. KG** Case C-453/21: **DPOs can't take decisions about personal data processing without breaching independence duties** FC had been the DPO of X-Fab since 1993. He was also the chair of the group's Works Council. In 2017, the group dismissed FC as DPO, on the basis that his role as chair of the works council was incompatible with his role as DPO. The dismissal was made at the request of the data protection authority for the relevant Laender. FC objected to this. The CJEU noted that GDPR specifically confirms that a DPO can have additional duties and obligations. However, this is only on the basis that these do not give rise to a conflict of interest. If the other duties involve the DPO in taking decisions about personal data processing, this would involve a conflict of interest. This would be a matter of fact, for national courts to determine.

Information Commissioner's Office (ICO)

Date	Description
December	**Tech Horizons Report** In mid-December, the ICO released its first annual Tech Horizons Report to establish its views on key emerging technologies, foster trust for personal data processing, and support innovation. The Report provides an in-depth analysis of four emerging technologies and outlines key privacy considerations and challenges for each of them: • **Consumer healthtech** – wearable devices and software applications that help people assess their health and wellbeing; • **Next-generation Internet of Things (IoT)** – physical objects that connect and share information, with the ability to sense, respond to or interact with the external environment; • **Immersive technology** – augmented and virtual reality hardware that creates immersive software experiences for users; • **Decentralised finance** – software that employs blockchain technology to support peer-to-peer financial transactions. A central theme underscoring each of these technologies is the broad collection of personal information. As the ICO stresses, while emerging tech promises to make lives easier, safer, and more comfortable, it also presents a range of risks that could harm privacy and trust. The Report identifies common challenges that apply to each technology and sets forth a list of goals centred around collaborating with the public, developing its Regulatory Sandbox with companies, drafting and issuing guidance, and monitoring market developments. The common challenges include non-transparent data collection, lack of user control over data processing, insufficient public and consumer awareness of how the technologies work and who to hold accountable for data-related harms, over collection of sensitive data such as biometric or health data, and enhanced tracking. The ICO intends to release similar reports going forward as part of its ICO25 Strategy. For more details on the report, see here

Other UK News

Date	Description
December	**Proposals to update the UK NIS Regulations** Following a consultation in 2022, the Department for Digital, Culture, Media and Sport has announced its intention to update the NIS regulations to improve the UK's cyber resilience. The changes come as part of a £2.6 billion National Cyber Strategy aimed at making the UK digital economy more secure and prosperous, whilst encouraging at-risk businesses to improve their cyber resilience. The UK Network and Information Systems ("NIS") Regulations (the "Regulations"), originally derived from the EU's NIS directive, and came into force in 2018 to improve the cyber security of companies providing critical services. "Critical services" include energy companies and the NHS, as well as important digital services like providers of cloud computing and online search engines. A reassessment of these laws took place in response to a string of high-profile attacks such as Operation CloudHopper, which targeted managed service providers. The legislative proposal seeks to expand the regulation of digital service providers ("DSPs") whilst future proofing the law. In summary, the proposals will: 1. **Expand the regulation of DSPs by bringing outsourced IT providers and managed service providers into scope to keep digital supply chains secure**. "Managed services" are defined to include those that are: a. supplied to a client by an external supplier b. involved in regular and ongoing management of data, IT infrastructure, IT networks and/or IT systems, c. B2B rather than B2C; and d. rely on NIS for their provision. A new risk-based approach is also proposed to limit the scope to the most impactful services. The ICO would be able to consider how critical providers are to supporting the resilience of the UK's essential services. The exemption on small and micro businesses (those with less than 50 employees) will be retained but modified to enable the ICO to designate specific small or micro DSPs within its scope where they are deemed systemically critical to the UK's critical services or national security. 2. **Establish a two-tier supervisory regime for DSPs**; proactive for those services that are most critical, and reactive for the rest. DSPs that are considered critical will be required to actively demonstrate compliance and appropriate

security measures to the ICO (with whom they must be registered). Non-critical DSPs must be ready to demonstrate this upon report of an incident.

3. **Give government the power to update the Regulations in the future to ensure they remain effective and enable new sectors and sub-sectors to be bought into scope** where they become vital to essential services or the UK's economy. It is anticipated that the government will address the issues raised during consultation around sufficient safeguards, limitations and parliamentary scrutiny.
4. **Allow regulators to designate critical sectoral dependencies in their supply chain for which their services rely on.** Respondents in the consultation called for guidance to address the necessity of stakeholder consultations as part of the designation process; ensure that regulators have the right and capability to monitor these organisations; and restrict unnecessary, disproportionate or inappropriate burdens to organisations. The government has agreed to reflect these points in the proposal.
5. **Additional incident reporting duties beyond continuity of service**, so that any incident that poses a significant risk to the security and resilience of the relevant entity is reportable to the regulator (i.e. Ofcom, Ofgem, ICO), even if it does not pose imminent disruption.
6. **Cost recovery provisions expanded to allow competent authorities to recover full costs**. The flexible 'hybrid' mechanism aimed at giving regulators more freedom to establish costs in a way that is more transparent and considers the wider regulatory burdens, size, and other factors**.** As this proposal received a critical reception at the consultation stage, it is uncertain exactly how the government's final approach on expanding cost recovery powers will be packaged.

The updates will be set out in legislation as soon as parliamentary time allows. Following this, further guidance is expected to clarify implementation, including how will the power to designate critical dependencies be used and what factors will be significant in assessing the need for the power to be used; what types of incidents must be reported and through which process; and the expected impact of the new cost recovery mechanism.

19 December

UK issues Adequacy Regulations in respect of South Korea

The Data Protection (Adequacy) (Republic of Korea) Regulations 2022 came into effect on 19 December 2022.

This is the UK's first decision to recognise a priority country as adequate post-Brexit. The decision demonstrates that each country is comfortable with the level of protection of personal data provided by the other and enables the transfer of data between countries without the need for contractual protections. This decision allows UK businesses to operate more seamlessly with partners in South Korea and reduces administrative and financial compliance costs that companies would normally face when transferring data overseas.

The European Commission granted an adequacy decision to South Korea in December 2021 however the UK's adequacy decision is broader than that of the EU. The most significant difference between the two is that UK organisations will be able to share personal data related to credit information with the Republic of Korea to help identify customers and verify payments.

UK ICO Enforcement

Date	Entity/Individual	Type of Breach & Sanction	Description of Breach
1 February	Mr Khan	Prosecution (unlawful obtaining of data)	Mr Khan, a former customer solutions employee of the breakdown services company, RAC, has been fined £5,000, ordered to pay court costs of £937.40 and a victim surcharge of £170 for a breach of s170 of the DPA 2018 for stealing data of victims of road traffic accidents. The RAC launched an internal investigation following the receipt of 21 complaints from suspicious drivers who had received calls from claims management companies following accidents which the RAC had been involved with. The investigation found that Mr Khan was the only employee who had access to these accident reports and he had been seen taking photos of his computer screen with this phone. A search warrant was executed by the ICO and two phones were seized from Mr Khan and a customer receipt for £12,000. The phones contained photos of data on it relating to over one hundred road incidents.
15 February	Its OK Limited	PECR: Unsolicited Marketing Calls £200,000 monetary penalty Enforcement Notice	The ICO issued an enforcement notice and fined It's OK Limited £200,000 for a "sustained and exploitative" campaign of nuisance calls potentially targeting many elderly people. The company, which is a nationwide appliance service and repair company, for domestic white good products, made over 1.7 million calls in a one year period to people registered with the Telephone Preference Service. It is currently against the law to make a live marketing call to anyone who is registered with the TPS, unless they have told the specific organisation that they do not object to receiving calls from them.
17 February	Martin Swan	Prosecution (unlawful obtaining of data)	The ICO has prosecuted and fined Mr Swan £630 plus accompanying court costs for unlawfully accessing the medical records of a child and his family.

Date	Entity/Individual	Type of Breach & Sanction	Description of Breach
			Mr Swan was working as a NHS 111 call adviser when he illegally accessed the records without consent or a legal reason to do so.

First-tier Tribunal Appeal Cases

Date	Appellant	Type of Case and Result	Summary of Case
4 January	**Collette Lloyd**	Appeals Dismissed	**Lloyd v Information Commissioner: Meaning of Personal Data [2023] UKFTT 00006** This decision concerned several appeals relating to the definition of "Personal Data" in the context of a number of similar Freedom of Information ("FOI") requests made concerning the number of live births with Downs syndrome in a particular NHS Trust's region per year. In each case, the NHS Trust had disclosed some information, but in regions where the number of live births was less than 5, the Trusts had declined to provide this data, citing an exemption under the Freedom of Information Act relating to this information being personal data under the UK GDPR. ***Background*** As there were a number of very similar requests, appeals directions were given in October 2019 that one particular appeal, Lloyd v Information Commissioner EA/2019/0285 (which concerned a request to Airedale NHS Foundation Trust), would be treated as the lead case. The decision in EA/2019/0285 was dated 11 February 2021 and the Tribunal upheld the decision notice in that case. Further directions were issued on 23 February 2021 that these appeals would be placed before a judge for consideration based on the decision of the lead case. However, before those appeals were put before the judge for further consideration, the Upper Tribunal gave another judgment in the case of *NHS Business Services v Information Commissioner and Spivack* from 6 August 2021 ("Spivack") which also dealt with the issue of what should be considered "personal data" and was considered relevant to these appeals as it reached a different conclusion. In Spivack, the Upper Tribunal reviewed the current case law and guidance and noted some uncertainties and ambiguities which needed to be explained and considered with care. Mr Justice Jacobs confirmed that the law creates a binary test as to whether something is personal data: "can a living individual be identified, directly or indirectly? If the answer is 'yes', the data is personal data. Otherwise, it is not." In so doing, the case noted that there was no mention of remoteness or likelihood- data could be personal data only if someone could say with

Date	Appellant	Type of Case and Result	Summary of Case
			certainty that the data related to a specific living person by combining that with other data reasonably available to them. In Spivack, this was applied to a data set consisting of a list of pharmacy dispensers who had supplied a particular drug, Stiripentol, through the NHS along with details of prescriptions, costs and quantities for each dispenser by month. The NHS had redacted the names and locations of the dispensers who had dispensed the drug fewer than five times in the relevant period, arguing that this would result in patients being identifiable; however, the Upper Tribunal concluded that this was not personal data as the data could not be linked to a person because a person known to take the drug may not appear on the list by reason of receiving the drug privately or through their hospital. As such, the FOI exemption did not apply. ***Decision*** However, by contrast, in the current case, the Tribunal considered that the correct test was to look at whether a 'motivated intruder' could identify a specific child from a data set e.g. by combining the withheld information with other available information which is the test used by the ICO. The Tribunal concluded that identifying a member of a data set in this way was possible. In doing so, they dismissed arguments that the requestor had no intention of making any such link, simply that a motivated intruder could do so, using the means that such a motivated intruder would be likely to use. Accordingly, this information was found to be personal data and the conclusion given in the lead case, EA/2019/0285 was correct and the same approach should be adopted with respect of the other appeals. ***Comment*** While the rejection of the ICO's guidance in Spivack is notable, Lloyd shows that the result is still in keeping with standard guidance here- in particular that the "motivated intruder test" is still the standard by which to consider whether data is identifiable, and that statements as to the intent or motivation of the particular requestor with regards to the data is irrelevant. . A link to the full case can be found here
16 January	**Robert Bartosik**	Application partially allowed	**Bartosik v Information Commissioner EA/2022/0065/GDPR**

Date	Appellant	Type of Case and Result	Summary of Case
			The Applicant (R) submitted a personal data erasure request on 24 March 2021 to Police Scotland. He was concerned about information held about him concerning his presence at Gorbals police station as he claimed he had never been in that police station. On May 9, 2021, the ICO received a complaint from R. Following the review of the complaint in August 2021, the ICO case officer advised Police Scotland that it had not complied with its data protection obligations in handling the erasure request and requested that Police Scotland responded to R as soon as possible. Police Scotland responded by saying that they had replied to R on 1 and 26 April 2021. Following a further review of the April correspondence, the case officer was satisfied that the request had been properly dealt with and no formal regulatory action would be taken. R requested a further case review. R then received a further letter from Police Scotland in February 2022 claiming that new information had come to light and that it was acknowledged that R had not been at Gorbals station and his original assertions were correct. Police Scotland confirmed that the information would not be deleted but instead would be restricted. On 15 March 2022, R wrote again to the ICO addressing this change in position from Police Scotland and complaining about further breaches of the Data Protection Act 2018. The case officer advised R that his complaint was the same as the original complaint and that there was no intention to reopen the case. R made an application to the Tribunal appealing this decision. The Tribunal held that the original complaint had been dealt with appropriately but it was wrong for the ICO to deal with the second complaint in the way that it had, given the new information which had come to light and the application was granted in this respect. The Tribunal ordered the ICO to respond to R's complaint appropriately and update R within 28 days of the decision as to its progress.
20th February 2023	**Experian**	Appeal upheld in part	**Experian v Information Commissioner, EA/ 2020/ 0317** The First-tier Tribunal overturned an Enforcement Notice served by the Information Commissioner on Experian. The Tribunal considered that Experian's current privacy notice is sufficient to meet UK GDPR requirements and rejected the Commissioner's conclusion that more was needed and that carrying out profiling to facilitate postal direct marketing, without more transparency, would cause distress. The Tribunal also allowed Experian to continue using credit reference agency data to suppress marketing of financial services products to individuals whose credit profile was such that any applications would be rejected. The Tribunal did require Experian to provide a privacy notice to 5.3 million individuals who would not have seen a

Date	Appellant	Type of Case and Result	Summary of Case
			privacy notice for the processing; this should not be considered a disproportionate effort; and if Experian considered this to be the case, then the correct approach would be to cease to undertake this business activity. Experian provides marketing services, in addition to operating a Credit Reference Agency. Once GDPR came fully into force, the Information Commissioner conducted an investigation into off-line direct marketing activities undertaken by all UK credit reference agencies. The Commissioner concluded that the processing carried out by Experian in this regard amounted to extensive profiling; that this would surprise individuals; that existing privacy information maintained by Experian was insufficient; and that Experian must actively provide a privacy notice to all individuals whose personal data it processed for this purpose. The Commissioner also argued that Experian's approach to legitimate interest was flawed and that certain of the processing carried out by Experian could only take place on the basis of data subject consent, not legitimate interests. Experian appealed against this. Hearings took place in January & February 2022. The First-tier Tribunal finally provided its decision on 20th February 2023. The First-tier Tribunal agreed that Experian's processing was large scale and, likely would be surprising to many people. However, it concluded that, as at the date of the decision, the privacy notice maintained by Experian on its website *was* sufficiently transparent and accessible [177]. The Information Commissioner had taken the view that, because the processing was surprising, Experian had an obligation to provide information about this more prominently. However, the Tribunal was sympathetic to the argument that provision of large amounts of information would actually cause information overload. It accepted that "*most people do not care what happens to their data"* and that layering is an effective way of dealing with this; and that those individuals who actually wanted to know more would be able to obtain this information by following through hyperlinks [165 – 169]. The Tribunal considered that the Information Commissioner had misunderstood the likely impact of Experian's processing. While the Commissioner considered it was likely to cause distress, the Tribunal considered that damage or distress was unlikely [187]. The Tribunal also considered that the Commissioner should have had regard to the fact that there was no adverse outcome for individuals and the economic and environmental impact of the proposed decision [184], [138]. The Tribunal also considered that the Commissioner's approach to use of credit reference agency data to prevent "over-marketing" was incorrect (i.e. to prevent products being offered to data subjects who would not be eligible for the product in question). The Tribunal accepted that there was a public interest in this

Date	Appellant	Type of Case and Result	Summary of Case
			processing [154], dismissing the Commissioner's concern that this would be seen as "stigmatising" by the individuals concerned as emotive [155]. The Tribunal did agree with the Commissioner that transparency was "foundational" [119]. During the hearings, Experian acknowledged that some 5.3 million data subjects would not have seen any privacy notice. The Tribunal substituted a new Enforcement Notice requiring Experian to identity these individuals and provide them with a notice within 12 months. The Tribunal specifically noted that, even though this would involve a significant business expense, this did not trigger the exemption from providing a notice in situations where this would be a "disproportionate effort". If the costs of compliance was considered too high, then Experian would be free to take the business decision not to carry on this part of the business [178]. The Tribunal also considered that Experian's practice of collecting data from third party data sources who had "consent" to share the data with Experian was problematic, on the basis that the consent would likely not have been sufficiently informed and so would have been invalid. However, as Experian had ceased this practice by the date of the decision no further action was needed [180]. The Tribunal noted that it was problematic that Experian continued to benefit commercially from personal data, previously processed unlawfully, because no notice had been given. It noted that this was still problematic even when the data was turned into anonymous models – because anonymisation is itself an act of processing which should be lawful. Here, however, the Tribunal concluded that it could not order steps that would be unclear or possibly incapable of implementation, so it – somewhat vaguely – asked Experian to consider what it could do to discontinue the processing [186]. It will be interesting to see if, in future cases, the Information Commissioner and the First-tier Tribunal look to the Federal Trade Commission's algorithmic disgorgement penalty as a way of addressing this topic.

Other News

Date	Description
14 December	**OECD Countries to limit government access to personal data** In December, Ministers and high level representatives of OECD Members and the European Union adopted the first intergovernmental agreement on common approaches to safeguarding privacy and other human rights and freedoms when accessing personal data for national security and law enforcement purposes. The Declaration, which rejects any approach to government access to personal data inconsistent with democratic values and the rule of law, is the result of two years of work by the OECD. This new Declaration articulates a set of shared principles that reflect commonalities drawn from OECD members' existing laws and practices. In particular, the principles set out how legal frameworks regulate government access, the legal standards applied when access is sought, how access is approved and how the resulting data is handled, as well as efforts by countries to provide transparency to the public. Moving forward, the principles in the Declaration will be implemented according to each country's legal framework. The Declaration is non-binding, but could assist companies to prove they are transferring data to a country with a heightened standard of protection of personal data.

Other recent articles/videos/tools

NIS 2 Directive, RCE Directive and DORA – Important EU cybersecurity-related legislative acts come into force
Third parties can now appeal Belgian DPA decisions before the Market Court
France: Publication of CNIL standards on health data processing implemented in the context of early access and compassionate use authorisations
Practical assistance from the Courts in relation to ransomware attacks: XXX v Persons Unknown (2022)
An Overview of the Implementation of the Whistleblowing Directive in the Nordics
How would the European Commission's new directive change AI-related liabilities?
Latest Updates to EU BCRs – what you need to know

Previous and upcoming events

How to prepare for the Swiss Data Protection Act

Recent legal directory rankings

Legal 500 UK - Tier 1, Data Protection, Privacy and Cybersecurity

"The B&B Privacy practice is top notch"
Great and responsive team with really unique and rare insight into the AdTech market from data privacy perspective."

Chambers UK - Band 1, Data Protection & Information Law

"They are a well-known, large, specialist and dedicated team doing a lot of work with leading tech clients"
"The firm has a strong international network, and its people are really knowledgeable and great to work with."

Ruth Boardman

Partner

+442074156018
ruth.boardman@twobirds.com

Ariane Mole

Partner

+33 (0)1 4268 6000
ariane.mole@twobirds.com

Elizabeth Upton

Legal Director

+442079056280
elizabeth.upton@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw