Bird & Bird

European Data Protection Bulletin

May 2022

Welcome to our regular European Data Protection Bulletin

In this edition, we bring you the following updates:

EUROPEAN UNION

EDPB

UNITED KINGDOM

ICO

UK Cases

UK Enforcement

ICO Enforcement

Information Tribunal Appeal Cases

EDPB

Date	Description
22 February	**EDPB issues finalised Guidelines on Codes of Conduct as tools for transfers** On 22 February 2022, the EDPB issued its Guidelines 04/2021 on Codes of Conduct as tools for transfers (the "**Guidelines**"). The Guidelines are intended to complement the EDPB's previous Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies - which establish the general framework for adoption of codes of conduct. The Guidelines state that the considerations set out in the 2019 Guidelines regarding admissibility, submission and criteria for approval of codes of conduct generally are also valid for the preparation of codes of conduct which are "intended for transfers" (i.e. intended to operate as an international transfer tool). Art. 40.2 GDPR envisages the drawing up of approved codes of conduct to assist with GDPR compliance by particular categories of controllers or processors. A recent example is the EU Cloud Code of Conduct for cloud service providers approved by the Belgian DPA last year. However, Art. 40.3 and 46.2(e) GDPR also envisage that approved codes of conduct can go further than simply being a general GDPR compliance tool and can operate as a transfer mechanism i.e. provide the "appropriate safeguards" which must be put in place for transfers of personal data to countries which do not provide an adequate level of data protection, much like standard contractual clauses and binding corporate rules. The stated aim of the Guidelines is to provide practical guidance on this latter type of code of conduct – their content and the process and parties involved, as well as the guarantees which such codes must provide if they are to work as a transfer mechanism (as detailed further below). The EDPB envisages that codes of conduct intended as a transfer tool can be used by organisations performing particular processing activities e.g. within a specific sector, or a common shared processing activity which shares the same characteristics and needs. A code of conduct intended for transfers would need to be adhered to by a data importer not directly subject to the GDPR located in a third country and then could be relied upon by a data exporter which is subject to the GDPR to legitimise its transfers to the data importer, without the data exporter having to adhere to the code itself.

The Guidelines state that codes of conduct being used as a transfer mechanism in this way must address both the essential principles, rights and obligations arising out of GDPR for controllers/processors (like any code of conduct) as well as guarantees that are specific to the transfer context (e.g. the issues of onward transfers, conflict of laws in the destination country etc.).

The Guidelines include a list of guarantees which must be provided under a code of conduct which is to be used as a transfer mechanism and which fall into two categories:

- Binding and enforceable commitments by controllers and processors which are not directly subject to the GDPR located in third countries to apply the "appropriate safeguards" provided by the code particularly as regards protecting and enforcing data subject rights – these commitments must be via a contractual or other legal binding instrument, and the Guidelines cover various contractual scenarios.

- Other elements such as description of the transfers covered by the code and the data protection principles to be complied with under the code, relevant accountability and transparency measures to be taken under the code, establishment of appropriate governance via DPOs or similar, and the existence of a suitable training program on the code's requirements, a data protection audit regime or other similar mechanism for monitoring compliance with the code and an appropriate complaint handling process where the code may not have been adhered to.

The Guidelines also detail the process to be followed for the adoption of codes of conduct intended to operate as a transfer tool (including a helpful flow chart detailing how a "transnational" code of conduct i.e. a code which covers processing activities in more than one EU member state is to be approved), and clarify the roles of the various parties involved in that process, namely the code owner, the code monitoring body, the relevant supervisory authority, the European Commission and, in the case of transnational codes, the EDPB.

14 March

EDPB Draft Guidelines on dark patterns in social media platform user interfaces

On 14 March 2022, the EDPB issued draft Guidelines on dark patterns in social media platforms – these were open to public consultation until earlier this month. The Guidelines do recognise though that dark patters are also relevant in other fields, particularly in the area of consumer protection, and it is likely that these Guidelines will also influence the approach in this area too.

The Guidelines, which are quite lengthy (64 pages), examine a number of dark patterns through examples and use cases and provide recommendations to designers and users of social media platforms on how to assess and avoid such practices. They also set out best practice recommendations for designing interfaces that facilitate the effective implementation of the GDPR.

What are "dark patterns"?

The EDPB defines "dark patterns" as interfaces and user experiences implemented on social media platforms that lead users into making *unintended*, *unwilling* and *potentially harmful* decisions regarding the processing of their personal data. Dark patterns aim to influence users' behaviour and can hinder their ability to effectively protect their personal data and make conscious choices.

Categories of dark patterns

The draft Guidelines identify and analyse 6 categories of dark patterns (see below) and specific types of dark patterns within each category. They also make another categorisation, distinguishing between "*content-based*" patterns, which refer to the actual content, the wording and context of the sentences and the information components, and "*interface-based*" patterns, which relate to the ways of displaying the content, navigating through it or interacting with it. The EDPB clarifies that this is a non-exhaustive list and other practices may well fall under the scope of dark patterns.

- ***Overloading:*** Burying users under a mass of requests, information options or possibilities in order to deter them from going further and make them keep or accept certain data practice. For example, making it particularly difficult for users to find out how to obtain certain information or exercise a data subject right ('*Privacy Maze'*) or providing users with too many options, leaving them unable to make any choice or making them overlook some settings (*'Too many options'*).
- ***Skipping:*** Designing the interface or user experience in such a way that users forget or do not think about all or some data protection aspects. For example, enabling by default the most data invasive features ('*Deceptive snugness'*) or putting a data protection related action or information in competition with another element, which could distract users ('*Look over there'*).
- ***Stirring:*** Affecting the choices users would make by appealing to their emotions or using visual nudges. For example, using wording/visuals that confers the information either in a highly positive outlook (making users feel good or safe) or in a highly negative one (making users feel scared or guilty) ('*Emotional steering'*). Also, using visual style for information or data protection controls that nudges users towards less restrictive/more invasive options ('*Hidden in plain sight*').
- ***Hindering:*** Hindering or blocking users in their process to obtain information or manage data, making the action hard or impossible to achieve. For example, not providing redirection links when users are looking for data protection information/controls or provide links that do not work ('*Dead end*'); or requiring more steps to activate a data protection control than the number of steps needed to activate data invasive options ('*Longer than necessary*').

• ***Fickle:***	Using an unstable and inconsistent interface design, making it hard for users to figure out where the different controls really are and what the processing is about. For example, presenting data protection information several times in several ways, so that users are likely to be confused ('*Lacking hierarchy*') or providing a data protection information/control on a page that is out of context ('*Decontextualising'*).
• ***Left in the dark:***	Designing the interface in a way that hides data protection information or controls or leaving users unsure of how their data is processed and what controls they have over it. For example, not providing data protection information in the official language of the country where users live and the service is offered ('*Language discontinuity*'); providing pieces of information that conflict each other in some way ('*Conflicting information*'); or using ambiguous and vague terms when giving information to users ('*Ambiguous wording or information*').

Social media lifecycle

The draft Guidelines examine how cases of the above dark pattern categories could arise throughout the life cycle of a social media account: from the sign-up process; the provision of information to users (including information about joint controllership or data breach communications), the provision of controls such as consent management and data protection settings; the provision of functions for the exercise of data subject rights; and through to the closure of a social media account.

How dark patterns interact with the GDPR?

The draft Guidelines note that the use of dark patterns in the social media sector could infringe a number of GDPR provisions. The fairness principle under Art. 5(1)(a) GDPR is the starting point to assess whether a design practice actually constitutes an infringing dark pattern, whilst the principles of transparency, data minimisation and accountability (and in some cases, purpose limitation) could also be relevant. Other GDPR provisions to which dark patterns could run contrary are the requirements for valid consent (Arts. 4(11) and 7 GDPR), data subject rights provisions, particularly Art. 12, and data protection by design and by default under Art. 25 GDPR.

The draft Guidelines point out that dark patterns raise additional concerns regarding potential impact on children, but do not expand on this further. Indeed, existing guidance on children's data, such as the ICO's Children's Code in the UK, or the DPC "Fundamentals for a child-oriented approach to data processing" in Ireland, examine practices that would fall under the EDPB's definition of dark patterns (e.g. nudge techniques).

Information Commissioner's Office (ICO)

Date	Description
February	**ICO issues updated Guidance on Video Surveillance** The ICO has issued new guidance for the use of video surveillance. The aim of the guidance is to bring it more in line with current surveillance technology used by the public and private sector. The guidance's main focus is on the use of CCTV (including a helpful CCTV checklist which can be accessed here), however further detail has been included to reflect the evolution of other surveillance technology (e.g. Facial Recognition Technology, ANPR, machine learning algorithms, dashcams and smart doorbells) and issues arising as a result. The key message is that there is an opportunity to build public trust and confidence whilst still realising the potential and benefits of new surveillance technology. Recognising the potentially intrusive nature of some of this technology, the ICO's view (perhaps unsurprisingly) is that trust is built when use of surveillance systems aligns with data protection law requirements such as accountability, lawfulness, fairness and transparency as well as proportionality. Examples include: • **Accountability** - implementing technical and organisational measures to show that the organisation has considered and integrated the principles of data protection law into its processing activities such as setting limits around the use of the system (incorporating measures to mitigate bias where needed), documenting procedures for use, access, storage, retention and destruction of the recordings and in certain instances completing an LIA or DPIA (e.g. for body worn cameras or facial recognition technology). • **Lawfulness, fairness and transparency** – ensuring that there is a lawful basis for use of surveillance systems. ICO notes that it will often be difficult to obtain genuine consent from individuals for processing their personal data in public spaces and here the appropriate lawful basis is most likely to be either legitimate interests, or public task (if you are a public authority); and ensuring the surveillance objectively aligns with people's reasonable expectations for instance when capturing large numbers of people (e.g. through signage and website notices when using drones) or when processing special category data such as biometric data (e.g. obtaining freely given consent for the use of facial recognition technology when the purpose is to uniquely identify the individual).

- **Proportionality** – ensuring that surveillance systems are not typically used to directly record conversations between members of the public (or to capture private conversations between employees) as this is highly intrusive and unlikely to be justifiable. Only processing the minimum amount of personal data needed to fulfil the specific purpose – this could involve recording for a defined time period or restricting the recording to a particular location.

The guidelines do not prescribe any specific minimum or maximum retention periods

There are practical tips on: recording virtual meetings, sharing surveillance footage with third parties and data subject rights. The guidance also acknowledges the wider regulatory framework and the impact for public authorities of obligations under FOIA, the Human Rights Act 1998 and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012.

For those who are otherwise exempt from the data protection fee, the use of surveillance systems can also trigger their need to notify and pay a data protection fee to the ICO.

The full guidance can be found here

February/March

ICO consults on two further chapters of its Anonymisation guidance

The ICO has been releasing its draft Anonymisation, Pseudonymisation and Privacy Enhancing Technologies (PETs) guidance chapter-by-chapter so that organisations can comment on a rolling basis, and is requesting feedback on all chapters with a consultation deadline of 16 September 2022. You can read our bulletin updates on Chapter 1 (Introduction to anonymisation) here and Chapter 2 (How do we ensure anonymisation is effective) here. We have set out a summary of the new Chapter 3 (Pseudonymisation) and Chapter 4 (Accountability and governance) below.

Chapter 3 – Pseudonymisation

The ICO is clear that pseudonymised data is still personal data and needs to be processed in compliance with the UK GDPR, unlike anonymised data which is no longer personal data and no longer subject to the UK GDPR.

ICO says that it is possible for the status of a dataset as "personal data" to change upon its disclosure to a different organisation, although circumstantial factors around likelihood of re-identification e.g. cost, time and information available, need to be assessed. For example, a pseudonymised dataset may remain personal data in the hands of Organisation A, but it may (depending on circumstances) be anonymous in the hands of Organisation B if it is disclosed without access to the key required to re-identify the individuals. This is consistent with the ICO's previous guidance, but contrasts with the Article 29 Working Party's Opinion on anonymisation techniques and the views of certain other European regulators.

The ICO emphasises that pseudonymisation is a beneficial security and risk mitigation measure; for example, it can reduce risks to individual rights, enhance security, make a notification requirement less likely in the event of a breach, and mitigate risk in the context of DPIAs and LIAs. In addition, the ICO explains how pseudonymisation can aid compliance with the purpose limitation principle and may permit organisations to conduct further "general analysis" on a dataset which may be more extensive than the analysis they could perform on anonymised data. The Chapter also considers the re-identification offences in the Data Protection Act 2018 and how organisations should approach pseudonymisation in practice.

Chapter 4 – Accountability and governance

Chapter 4 has a more practical focus on the accountability and governance measures organisations need to consider when anonymising personal data. The key areas of the ICO's suggested governance structure (which the ICO says should be "comprehensive") include:

- **Planning for anonymisation –** an individual or group of individuals of sufficient seniority (e.g. a Senior Information Risk Owner or "SIRO") should oversee the process and should work closely with the DPO if applicable.

- **Identifying and mitigating risks –** a DPIA can be a useful tool to assess risk and structure decision-making, and will be mandatory in an anonymisation context where there is (i) use of innovative technology (e.g. differential privacy) or (ii) matching data or combining of datasets from different sources. If planning to disclose any anonymous information, organisations should work with third parties (e.g. those processing or disclosing other information which could be used to re-identify the original organisation's information and impact the effectiveness of their anonymisation) to assess risks collectively and agree mitigations and the use of TTPs (trusted third parties) should be considered. Organisations should be clear about their reasons for anonymising, what sort of disclosure will be made (e.g. limited or open release) and how to safeguard accordingly, and how to deal with cases with high re-identifiability risk. Transparency information about anonymisation should be provided to data subjects to promote trust.

- **Ensuring anonymisation remains effective –** organisations should keep up to date with legal and technological developments, and ensure staff (in particular key decision-makers) are trained on this. Re-identification risk should be assessed on an ongoing basis.

- **Accounting for other legal considerations** – the implications of other laws (e.g. the Freedom of Information Act 2000 and the Human Rights Act 1998) and common law rules around confidentiality may need to be considered.

If a security incident leads to re-identification, the ICO says this would not be considered a personal data breach provided that organisations can demonstrate their decision-making to justify that data was effectively anonymised. This can be done through (i) following the good practice in the Chapter and (iii) documenting how it was used to mitigate risks to individuals.

Remaining chapters

The remaining chapters to be released over the coming months are as follows:

- Anonymisation and research - how anonymisation and pseudonymisation apply in the context of research;
- Guidance on privacy enhancing technologies (PETs) and their role in safe data sharing;
- Technological solutions – exploring possible options and best practices for implementation; and
- Data sharing options and case studies – supporting organisations to choose the right data sharing measures in a number of contexts including sharing between different organisations and open data release.

April

ICO issues draft Guidance on Research

In April 2022, the ICO closed a consultation into its new proposed guidance on the research provisions in the UK GDPR and the DPA 2018.

The draft guidance is available here.

How is research defined?

There is no definition of 'research' in UK data protection law, the law covers three areas: (i) archiving purposes in the public interest; (ii) scientific or historical research; and (iii) statistical purposes. The ICO commits 9 pages to an analysis of what these cover, noting in particular, that scientific research purposes should be "*understood broadly*" and that this extends beyond traditional academic settings – which is likely to be welcome for commercial R&D as well as for those working on AI which may have multiple, including commercial, applications.

The guidance provides a set of indicative criteria (with examples) for research of which the ICO would expect more than one to be met. The criteria are categorised into activities (e.g. observation, peer review), standards (e.g. ethics guidance and committee approval) and access (e.g. publication of results).

What are the research provisions?

The research provisions are scattered through the UK GDPR and DPA 2018 and address:

- lawful bases for processing;
- purpose limitation and re-use of data;
- storage limitation;
- lawful bases for processing; and

- data subject rights.

Data protection requirements are also particularly relevant to transparency, and data sharing, although there is no 'special regime' covering these points.

The draft guidance provides a table of these provisions which maps where they sit in the legislation (at page 5).

Lawful basis for research processing, and the problem with consent

The draft guidance explains that where processing personal data for research purposes, the most appropriate lawful basis is likely to be either:

- for the public sector – public task (Article 6(1)(e); or
- for the private and third sector – legitimate interests (Article 6(1)(f)

As for consent, the ICO states that "*in most cases, consent will **not** be the most appropriate lawful basis*".

The guidance also clarifies that consent to participate in a research study is distinct from, and not to be confused with, consent as a lawful basis under data protection law.

Re-use of personal data for research purposes

Personal data collected for one purpose cannot be further processed for another purpose that is incompatible. The draft guidance clarifies that the operation of Article 5(1)(b) UK GDPR means that research related purposes should be considered compatible with the original purpose. This has two important qualifications:

- according to the draft guidance, it does not apply when the original basis was consent. In these cases to process data for a new research purpose, fresh consent is needed.);
- it does not apply where you are conducting research using data collected from another organisation. This would be considered 'new' rather than 'repurposed' data.

Special category data

Where the personal data being used for research is of a special category, such as health, an Article 9 condition must be met in addition to an Article 6 legal basis. Article 9(2)(j) provides a condition where the processing is necessary for scientific research in accordance with Article 89 UK GDPR. This is supplemented by additional criteria in Schedule 1, Paragraph 4 of the DPA 2018.

For those criteria to be met:

- **processing must be necessary** – that this "*does not mean that the processing has to be absolutely essentially*" but that it must be a "*targeted and proportionate way of achieving that purpose*".
- **processing must be not likely to cause substantial damage or substantial distress** – distress must be "*beyond annoyance, irritation, strong dislike, or a feeling that the processing is morally abhorrent*".
- **there must be a public interest** – this "*should be interpreted broadly to include any clear and positive benefit to the public likely to arise from that research*". The ICO gives examples such as improved health and wellbeing outcomes, advancement of academic knowledge, and the provision of more efficient or more effective products and services for the public.
- **there must be appropriate safeguards in place** – the draft guidance goes into little detail here in comparison to other areas, but refers to its forthcoming guidance on anonymisation, pseudonymisation and privacy enhancing technologies.

The draft guidance also confirms that for the condition to apply, the processing should not be used for measures or decisions about particular individuals, except in the case of approved medical research (e.g. clinical trials).

Transparency

Where research data is collected indirectly, Article 14(5)(b) UK GDPR provides an exception (which is not research specific) where the provision of a notice would prove impossible or require disproportionate effort.

The ICO says that the exception is not automatic and requires a balancing exercise, where you must consider:

- the number of data subjects (e.g. it would be easier to justify not providing a notice where the dataset is very large);
- the age of the data; and
- any safeguards

If the exception applies, then you would still be required to publish a privacy notice online, and the draft guidance requires you to conduct a DPIA.

UK Cases

Date	Description
2 March	**Brake v. Guy [2022] EWCA Civ 235: Employee had no reasonable basis to expect privacy in respect of personal emails sent using a shared work account** On 2 March, the Court of Appeal handed down its decision in *Brake v Guy*, which concerned an appeal against an order dismissing a claim by Nihal and Andrew Brake against Dr Guy and some of his companies alleging the misuse of private information and breach of confidence. The private information in question was contained in emails sent and received by one of the claimants via an email account which was set up and operated by one of Dr Guy's companies. The account in question was an enquiries inbox (i.e. enquiries@axnoller.co.uk), and the employees who had access to this account were also provided with their own personal accounts (i.e. *firstname*@axnoller.co.uk). The judge held that the claimants had no reasonable expectation of privacy and no right of confidentiality in respect of emails contained within the enquiries inbox. The claimants appealed arguing that the law had not been correctly applied to the facts as found. The Court of Appeal rejected the claimants' arguments and upheld the initial ruling in favour of Dr Guy and his companies, that decision there was no reasonable basis to expect privacy or confidentiality for personal emails sent and received using the work account provided by the companies. The judgment provides a helpful summary of the law of misuse of private information, and a summary of factors that would determine whether an employee might have a reasonable expectation of privacy in relation to workplace emails and other uses of workplace IT systems. The law of misuse of private information The judgment provides a helpful summary of the law of misuse of private information, namely: • *Campbell v MGN Ltd* [2004] UKHL 22 identifies the tort of misuse of private information which consists of two components, (i) whether there is a "reasonable expectation of privacy" giving rise to the Art 8 ECHR right and (ii) whether there has been an unjustified interference with this qualified right; • in considering whether an expectation of privacy is reasonable, various factors should be considered, including the attributes of the claimant, the nature of the activity in which the claimant was engaged, the place at which it was

happening, the nature and purpose of the intrusion, the absence of consent and whether it was known or could be inferred, the effect on the claimant and the circumstances in which and the purposes for which the information came into the hands of the publisher (Relevant cases cited included: *Murray v Express Newspapers PLC* [2008] EWCA Civ 44, [2009] Ch 481), *In re JR28* [2015] UKSC 42, [2016] AC 1131 and *Bloomberg LP v ZXC* [2022] UKSC 5);
- there is no presumption of privacy in information, it is for the claimant to demonstrate that the information is private (*Bloomberg);* and
- in establishing whether the right has been interfered with, the right to privacy must be balanced against the competing right (usually the right to freedom of expression) (*McKennitt v Ash* [2006] EWCA Civ 1714, [2008] QB 73). Neither right has preference over the other; the focus should be the comparative importance of the rights in a particular case; justifications for interfering with the right should be considered; proportionality must be considered (*PJS v News Group Newspapers Ltd* [2016] UKSC 26, [2016] AC)

Demonstrating a misuse of private information

Following the recent Supreme Court decision in *Bloomberg V ZXC [2022] UKSC 5,* Baker LJ considered that there was a burden on the claimants to demonstrate the confidential nature of the information and that the appellants' grounds for appeal wrongly implied an inversion of the burden of proof. He further observed that the approach to demonstrating the confidential nature of the information was also insufficient: the claimants had defined sixteen categories of email, ten of which were argued by the claimants to be *manifestly private* therefore giving rise to a reasonable expectation of privacy. Baker LJ found two issues with this analysis: firstly, the claimants had provided insufficient documents to support their assertion (having provided only two of 3,149 emails); and secondly, even if the emails were confirmed to be private in nature, this was not a decisive factor and was only one of a variety of factors that ought to be considered in reaching a conclusion about whether a reasonable expectation of privacy had arisen. The judge's findings at the interim injunction were clarified as being interim and bore no weight in the appeal.

Factors undermining a reasonable expectation of privacy

Baker LJ recognised and cited key authorities which confirm that an employee making a private communication from business premises or using business facilities may have a reasonable expectation of privacy (*Halford v United Kingdom* [1997] IRLR 471, *Copland v United Kingdom* (2007) 45 EHRR 37, and *Barbulescu v Romania* (Application no. 61496/08) [2017] IRLR 1032), and that an employer's express ban on using company resources for personal purposes and monitoring of internet use "*cannot reduce private social life in the workplace to zero*." (*Barbulescu*). He distinguished the facts in front of him and listed the following factors which undermined a reasonable expectation of privacy in this case:

- notably, that the claimant shared access to the account with two others;
- at the time the shared email account was set up, personal accounts were set up for all those who had access to it;

- the nature and purpose of the account – the account was a business account intended to receive enquiries from customers and potential customers;
- the account belonged to the company and was intended to protect the secrets of the company, not the secrets of the individuals;
- the claimant did not have access to the email address when it was set up, her access to the email was provided in her capacity as an employee;
- the company owned the domain and had access to and administrative control over the account;
- there was no segregation of the allegedly private emails in the account – it would be impossible to tell which emails were "private" without reading them; and
- misconduct is likely to undermine an expectation to privacy.

Further factors that were considered particularly important when considering whether an employee should have an expectation against his employer in the context of workplace emails included:

- whether the employee was on notice that such access was taking place (for example, by signing an IT policy stating that emails sent on company systems were the property of the company;
- the circumstances in which the document was created (e.g. on company software and using company information);
- whether the document was password protected or segregated from other work documents;
- where the document was stored;
- who else had access to the documents; and
- crucially, whether the individual had demonstrated a right to privacy against the employer.

UK ICO Enforcement

Date	Entity	Type of Breach & Sanction	Description of Breach
17 February	**The Money Hive Limited**	PECR (Reg 22) Monetary Penalty of £50,000 Enforcement Notice	The ICO fined and issued an Enforcement Notice against the Money Hive Limited (TMHL) for sending direct marketing text messages without consent. Between 12 March 2020 to 8 September 2020. TMHL sent 752,425 unsolicited direct marketing text messages promoting high interest payday loans, which resulted in 1,360 complaints. The messages had been sent to individuals who had previously applied online for a loan with a TMHL operated website but where the individuals had failed to proceed with the loan. TMHL tried unsuccessfully to argue that the messages were service messages but given that they advertised the availability of loan products from both TMHL and third party providers, the ICO disagreed. Whilst TMHL did provide a separate set of optional opt-in boxes for individuals who might wish to agree to marketing in the future, if a subscriber wished to proceed with their online loan application, they were required to agree to receive an undefined number of contacts (telephone, email and text message) from TMHL and a range of third-parties which in itself, required consent. As such, the Commissioner concluded that TMHL had not obtained valid consent for sending the text messages and suggested that TMHL should have had separate elements to its opt-in page i.e., by making agreement to the credit check and use of its online loan application process separate and distinct from its request for individuals to agree to follow-up direct marketing communications. Furthermore, the soft opt-in exemption provided by Regulation 22(3) of the PECR was not available as individuals were unable to opt-out since agreement to receipt of these messages was a condition of service. In determining the monetary penalty, the fact the direct marketing is likely to have been sent to vulnerable individuals in financial difficulty was seen as an aggravating factor. No mitigating features were considered to be present.

7 March 2022	**Smith, Law & Shepherds IFA Ltd**	GDPR (Article 15) Enforcement Notice	The ICO issued Smith, Law & Shepherds IFA Ltd with an Enforcement Notice requiring the company to respond to two subject access requests. This related to requests which had been made by two data subjects on 14 and 17 April 2020 respectively, which had asked for "a copy of all documents, of any kind, which relate to me and my pension", under the Data Protection Act 2018. After receiving no response, the two data subjects complained to the ICO. The ICO called the firm multiple times, but no information had been received by either individual by December 2021, almost a year and a half after their initial requests. This prompted the ICO to issue an Enforcement Notice.
8 March 2022	**Royal Mail Group Limited**	PECR (Reg 22) Monetary Penalty of £20,000	The ICO fined Royal Mail Group Limited ("RM") £20,000 for accidentally sending a direct marketing email to multiple parties who had opted-out. On 27 April 2021, 215,202 parties unintentionally received a direct marketing email from RM as a result of a technical error, despite having expressed a desire to no longer receive marketing messages. As soon as RM discovered that this had happened, it submitted a breach report to the ICO on 29 April 2021 in the knowledge that this particular marketing campaign might have breached the PECR. RM were subsequently sent an initial investigation letter by the Commissioner on 3 June 2021, to which they replied with a copy of the marketing email that was sent. RM also confirmed that the cause was a manual error and explained it had since implemented a number of measures to minimise the potential for reoccurrence. Whilst the Commissioner considered that RM had indicated it would undertake an internal Data Protection audit, it was an isolated incident of human error and that RM had cooperated in reporting the incident, the Commissioner nevertheless determined that imposing a monetary penalty should act as a general encouragement towards compliance. The Commissioner also took into account the six responses / complaints received by RM from individuals who had opted-out and the fact that RM had already received a monetary penalty notice of £12,000 from the ICO for another contravention of Regulation 22 PECR in 2018.
10 March 2022	**Tuckers Solicitors LLP**	GDPR (Article 5(1)(f)) Monetary Penalty of £98,000	The ICO fined Tuckers Solicitors LLP ("Tuckers") £98,000 for failing to process personal data in a manner that ensured appropriate security of personal data. On 24 August 2020, Tuckers became aware of a ransomware attack on its systems which resulted in a personal data breach and encryption of 927,191 files (of which 24,712 related to

			court bundles) and 60 court bundles being exfiltrated by the attacker and released in underground data marketplaces. The 60 court bundles included sensitive personal data such as medical files, names and addresses of victims and witnesses, and the alleged crimes of individuals. Tuckers reported the personal data breach to the ICO the next day, on 25 August 2020, and updated the Commissioner on 7 September 2020 that they were unable to restore the compromised data and that the court bundles were effectively permanently lost. Although the ICO accepted primary culpability for the incident lay with the attacker, between 25 May 2018 (when GDPR came into effect) to 25 August 2020, Tuckers were found to have failed to process personal data in a manner that ensured appropriate security, given the volume and nature of the personal data being processed. In particular, Tuckers did not install a patch update that became available in January 2020 until June 2020, leaving an exploitable five-month period; failed to use multi-factor authentication; and did not encrypt personal data, all of which could have mitigated some of the risks posed to the affected data subjects. The Commissioner determined that Tuckers had contravened Article 5(1)(f) by failing to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Additionally the ICO raised concerns over Tuckers compliance with Articles 5(1)(e), 25, 32(1)(a) and 32(1)(b) GDPR during the relevant period (although this did not form the basis of the substantive breach). The nature of the infringement, negligence, mitigating action, responsibility, the type of data effected and the fact that Tuckers self-reported the breach were all considered in the monetary penalty.

On the 15 March 2022, the ICO announced fines totalling £405,000 to five companies responsible for making over 750,000 unwanted marketing calls targeted at older, vulnerable people. The companies had each specifically bought marketing data lists from third parties for individuals aged 60 and over, who were homeowners with landline numbers. All companies were also issued with Enforcement Notices that required them to stop making the predatory calls.

16 March 2022	**UK Appliance Cover Limited**	PECR (Regulations 21 and 24) Monetary Penalty of £100,000 Enforcement Notice	The ICO fined UK Appliance Cover Limited ("UKACL") for making unsolicited calls for direct marketing purposes and failing to provide the necessary caller information. The ICO also issued an Enforcement Notice ordering UKACL to stop making further calls of this type. The Commissioner sent several investigation letters to UKACL between 2 September 2020 to 26 November 2020, after reviewing complaints from individuals suggesting UKACL were making aggressive, threatening, unsolicited direct marketing calls targeting vulnerable individuals for financial gain. UKACL ignored the investigation letters as well as an information notice served on 26 November 2020.

			On 7 January 2021, the Commissioner obtained a copy of UKACL's Call Detail Records between 1 June 2020 and 31 December 2020. The records showed that 39,167 calls had been made to people registered with the Telephone Preference Service ("TPS"). UKACL subsequently ignored several further information notices, failed to provide any evidence that the subscribers who had received these calls had indicated they did not object to such calls, nor did they provide the recipient with the necessary caller information. The ICO also found no evidence that the services advertised through the nuisance calls were actually being provided. In determining the monetary penalty, the Commissioner considered aggravating factors such as the targeting of vulnerable individuals, attempting to gain an advantage over businesses that comply with PECR and failure to co-operate with the ICO. The Commissioner did not find any mitigating factors in the case.
16 March 2022	**Home Sure Solutions Limited**	PECR (Regulation 21) Monetary Penalty of £100,000 Enforcement Notice	The ICO fined Home Sure Solutions Limited ("HSSL") for making unsolicited calls for direct marketing purposes. The ICO also issued an Enforcement Notice ordering HSSL to stop making further calls of this type. Between 3 March 2020 to 30 September 2020 HSSL made 229,483 unwanted marketing calls relating to home emergency cover to people registered with the Telephone Protection Service ("TPS"). This came to the attention of the Commissioner in September 2020 following several complaints. Concerned about HSSL's practices, the ICO sent an initial investigation letter, followed by a chaser, in December 2020 and January 2021 respectively. HSSL did not respond, so the ICO served an Information Notice on 26 January 2021. HSSL responded on 1 March 2021 stating that they purchased the data from a third-party data provider and relied on them to have obtained consent for the calls. HSSL also claimed that it did not screen for TPS as they had requested the third-party screen the data prior to HSSL purchasing it. As evidence, HSSL provided some screenshots of emails between itself and the third-party data provider from February 2020 regarding the purchase of data and TPS checks. These revealed that HSSL were deliberately targeting older people as they were provided with prices matching their "criteria" of UK Homeowners, aged 60+, and landline numbers. The Commissioner sent some follow-up queries, requesting evidence of (i) the "consent statements" provided to individuals when their data was collected, (ii) due diligence conducted on the third-party data provider, and (iii) a contract / purchase agreement with the third-party data provider. HSSL said it did not have copies of consent statements and said it had done due diligence by asking for confirmation that the third-party had obtained the information correctly

			and followed guidelines. It did not have a contract with the third-party and instead said it would be invoiced for the data it purchased, despite not providing an invoices as evidence. The Commissioner said it expected evidence of consent to be obtained by HSSL as part of its due diligence before relying upon this evidence for its direct marketing campaign. HSSL therefore failed to provide any evidence that (i) the parties had given consent to receive marketing calls from HSSL, and (ii) it had undertaken due diligence in respect of the data which it was choosing to purchase. In determining the monetary penalty, the Commissioner took into account aggravating factors such as 'pressured sales tactics', the contravention of PECR to gain an unfair advantage over competition who complied with legislation and the targeting of vulnerable groups (60+).
16 March 2022	**Seaview Brokers Limited**	PECR (Regulation 21) Monetary Penalty of £15,000 Enforcement Notice	The ICO fined Seaview Brokers Limited ("Seaview") for making 4,73 unsolicited calls for direct marketing purposes to vulnerable people. The ICO also issued an Enforcement Notice ordering Seaview to stop making further calls of this type. On 21 August 2020, the ICO sent an initial investigation letter to Seaview after receiving complaints from people registered with the Telephone Protection Service ("TPS"). Seaview responded that they had purchased a data book from another company, preventing customers losing out on contracts already paid for. They said they did not engage in outbound marketing calls and believed they were entitled to contact customers it had purchased via the data book. However, Seaview was unable to provide evidence that it had consent for the direct marketing or that it had carried out due diligence. It was therefore determined that 4,737 unsolicited calls were made between 1 June 2020 to 30 June 2020 by Seaview for direct marketing purposes. In determining the monetary penalty, the Commissioner took into account aggravating factors such as the type of marketing used to aggressively target vulnerable individuals, the gaining of an unfair advantage over competition who were complying with the PECR and the lack of documents kept by Seaview in regards to the purchase of the direct debit book / database. Seaview has lodged an appeal with the First-Tier Tribunal (General Regulatory Chamber).
16 March 2022	**Domestic Support Ltd**	PECR (Regulation 21 and 24)	The ICO fined Domestic Support Ltd ("DSL") for making 69,133 unsolicited calls between 1 January 2020 to 31 July 2020 for direct marketing purposes to subscribers who were registered with the Telephone Protection Service ("TSP") without having valid consent, and for failing to

		Monetary Penalty of £80,000 Enforcement Notice	provide necessary caller information. The ICO also issued an Enforcement Notice ordering DSL to stop making further calls of this type. DSL responded to the investigation correspondence claiming that the data had been bought from third-party data providers who had carried out TSP checks, this was then compared to an in-house suppression list and put through a paid-for online TPS screener. Further, they stated that they no longer made sales or marketing calls and the only calls made were to existing customers. However, the Commissioner's investigation found that DSL was unaware of precisely where the data it purchased was from and was unable to provide a contract with the third-party data provider, details of the Call Line Identity ("CLI") used or consent statements from the parties contacted. Further, complaints suggested DSL was providing different trading names when calling people, which is unlawful. The Commissioner took into account aggravating features such as purchasing records specifically for vulnerable individuals (aimed between 55 and 75), gaining an unfair advantage over competition who were complying with PECR and a failure to thoroughly answer the Commissioner's questions.
16 March 2022	**UK Platinum Home Care Services Limited**	PECR (Regulation 21) Monetary Penalty of £110,000 Enforcement Notice	The ICO fined UK Platinum Home Care Services Limited ("Platinum Home Care") for making unsolicited calls for direct marketing purposes. The ICO also issued an Enforcement Notice ordering Platinum Home Care to stop making further calls of this type. Platinum Home Care is a company which offers a range of policies for home appliances such as boiler, central heating and electrical appliance breakdown cover. After reviewing several complaints, the Commissioner sent a letter raising concerns over compliance with the PECR in October 2020. A lawyer responded, on behalf of Platinum Home Care, confirming that they did not routinely screen calls to UK numbers against the TPS but did operate an internal suppression list and that staff underwent training. However, after investigation, it was found that of the 1,789, 786 unsolicited direct marketing calls made over a 7-month period, 412,446 calls were answered by TPS registered individuals who had not notified Platinum Home Care that they were willing to receive such calls. Furthermore, there was clear evidence the company had purchased personal data from third-party providers, requesting the landline numbers of homeowners aged 60-80. As such this was a serious contravention as Platinum Home Care had failed to screen the calls against the TPS register, conduct proper due diligence and had targeted people over the age of 60. Moreover, there was clear evidence of distress caused to at least one victim.

			The breach was also deliberate and negligent; Mr Govender, Platinum Home Care's director, was found to be ignorant of the UK regulations at the time the calls were made. In determining the monetary penalty, the Commissioner took into account Platinum Home Care's engagement with the investigation, the fact that they did not attempt to evade regulatory action and that the company has committed to taking steps to ensure future compliance, despite several aggravating factors. Platinum Home Care has lodged an appeal with the First-Tier Tribunal (General Regulatory Chamber).
31 March 2022	**H&L Business Consulting Limited**	PECR (Regulation 22 and 23) Monetary Penalty of £80,000 Enforcement Notice	The ICO fined H&L Business Consulting Limited ("H&L") for sending unsolicited SMS messages for direct marketing purposes. ICO also issued an Enforcement Notice ordering H&L to stop sending further SMS messages of this type. The company sought to capitalise from the pandemic by directly referencing lockdown and promoting "government-backed" debt management schemes despite H&L not being FCA authorised. It was determined that between 20 January 2020 to 27 July 2020, H&L had sent 451,705 unsolicited SMS messages (378,538 were delivered) for direct marketing purposes to people who had not consented to receiving them. Mr Gray, H&L's sole director (who had failed to cooperate with the ICO previously) was unable to supply the Commissioner with substantive information when requested. After conducting further investigations, the Commissioner was able to gain information from a third-party revealing that Mr Gray had purchased and sent bulk SMS messages from H&L. After multiple delays and requests for additional time, Mr Gray failed to respond to the information notice and the ICO concluded its investigation. In determining the monetary penalty, the Commissioner took into account aggravating factors such as H&L concealing their identity in contravention of Regulation 23 PECR, the motivator of financial gain, Mr Gray's history of non-compliance and his conduct frustrating the ICO's investigation. H&L had also adapted its content and changed its email address indicating poor regulatory compliance.
8 April 2022	**Bizfella Limited**	PECR (Regulation 22) Monetary Penalty of £30,000	The ICO fined Bizfella Limited ("Bizfella") for sending unsolicited SMS messages for direct marketing purposes. The ICO also issued an Enforcement Notice ordering Bizfella to stop making further messages of this type.

		Enforcement Notice	Bizfella is an FCA registered credit broker where individuals, via a website, can submit loan applications, which are then passed on to a panel of lenders to be approved or declined. The outcome of an individual's loan application would be passed on by an SMS message. Bizfella would then send direct marketing messages to that number encouraging the individual to apply for a loan again via the website. On 15 July 2020, the Commissioner sent an investigation letter explaining its concerns about the SMS marketing campaign following 906 complaints in response to SMS advertisements. On 29 July 2020, Bizfella replied to the Commissioner providing information of the number of SMS messages sent and the third-party service provider used. Bizfella claimed that all of the SMS messages were consented to by users of the website. On 13 November 2020, a meeting was held between Bizfella and the ICO. Bizfella stated multiple websites were used to collect the data, the SMS messages were only sent to those who had applied through the service, and Bizfella relied upon "first party consent". The Commissioner determined that Bizfella had incorrectly relied upon a statement and tick box that was included on its websites at the time an individual applied for the initial loan as constituting consent and/or satisfying the soft opt-in rule. However, this box had to be ticked to submit a loan application, which meant valid consent had not been obtained as there was no real choice or control given. Further, the statement on the website referred to contact "in relation to the applications", which did not inform the individual that they were going to receive marketing messages. Therefore, it was determined that between 15 November 2019 to 15 June 2020, Bizfella instigated the sending of 224,550 unsolicited direct marketing SMS messages without having valid consent. In determining the monetary penalty, the Commissioner took into account aggravating factors such as the fact that there had been deliberate action for financial gain from Bizfella and the fact that Bizfella had not acted on guidance or advice given to them by the Commissioner.
13 April 2022	**Finance Giant Ltd**	PECR (Regulation 22 and 23) Monetary Penalty of £60,000	The ICO fined Finance Giant Limited ("FGL") for sending unsolicited messages (SMS and emails) for direct marketing purposes during the pandemic to generate additional customers and profit. Between 1 to 30 November 2020 FGL sent 505,759 unsolicited direct marketing messages. There were (i) 40,524 direct marketing SMS sent and 27,608 direct marketing SMS received by

			subscribers; and (ii) 465,235 direct marketing emails sent and 445,138 direct marketing emails received. FGL had relied on "consents" to direct marketing as part of their application process. However, the Commissioner found that this only enabled applicants to signify their agreement to the terms & conditions as applicants were not informed that direct marketing messages would be sent unless they consulted the terms of FGL's privacy policy. There needed to be a separate opt-in or opt-out box to enable applicants either to consent or withdraw consent specifically in relation to direct marketing messages. Additionally, the Commissioner found that the 27, 608 direct marketing SMS did not contain any opt-out for individuals to stop receiving further messages. The conduct was considered deliberate, even if Finance Giant did not actually intend to do so. In determining the monetary penalty, the Commissioner considered the aggravating factor of FGL's motivation to increase its customer base during the pandemic and generate additional profit; they also considered mitigating features such as FGL ceasing electronic marketing following notification of the Commissioners investigation and that FGL indicated it had taken legal advice to ensure further and ongoing compliance.
22 April 2022	**Reed Online Limited**	PECR (Regulation 22) Monetary Penalty of £40,000	The ICO fined Reed Online Limited (ROL) for unsolicited direct marketing emails without valid consent. Between 4 to 7 February 2021 a total of 6,205,966 emails were sent with direct market materials which subscribers had not provided valid consent for. ROL asserted there was no intention to send the email for purposes of direct marketing. The Commissioner acknowledged that the email was sent due to human error, however it found that intention is not a necessary element to contravene the regulation and the high number of individuals affected made the contravention serious. Whilst ROL did not deliberately seek to contravene, it did have a high proportion of opt out clients. Therefore, its lack of preventative measures and inadequate checks means ROL failed to take reasonable steps to prevent the contraventions, making it negligent.

Information Tribunal Appeal Cases

Date	Appellant	Type of Case and Result	Summary of Case
29 March	**James Peters**	Appeal against the imposition of a monetary penalty for failure to pay the £60 data protection fee. The Appellant tried (unsuccessfully) to argue that the ICO emails and reminders were sent to an out of date address.	Appeal Reference: EA/2021/0307/FP Appeal dismissed and penalty upheld.

Other recent articles

- International Comparative Legal Guide to Digital Health 2022
- Q&A with Financier Worldwide on the evolution of the automotive sector – disruption
- The impact of the EU digital initiatives on the creation, exploitation of and access to digital rights and assets
- Is the European Data Protection Board a pioneer for product innovations based on Artificial Intelligence/Machine Learning?
- SLOVAKIA: Cookies Under the New Electronic Communications Act
- SLOVAKIA: New Electronic Communications Act
- SLOVAKIA: Direct Marketing and unsolicited communications
- SPAIN: The right to privacy: not everything goes
- AUSTRALIA: Australian data breach class actions
- CHINA: China Cybersecurity and Data Protection: MIIT Pioneers its Data Security Regime
- CHINA: China Cybersecurity and Data Protection: Monthly Update - March 2022 Issue
- CHINA:China Cybersecurity and Data Protection: Monthly Update – April 2022 Issue
- CHINA: Employee Data Protection Series (VI): Processing Employees' Personal Information During and After Separation Management

Previous events

- **Thursday 5th May 2022 - Cyber Threat and Legal Landscape: A"Birds Eye View"** – view recording of webinar here.

This webinar brings experts from CrowdStrike's Falcon threat intel team and Bird & Bird lawyers will provide a "birds eye view" of the current cyber threat and legal landscape resulting from the latest nation-state, eCrime threat activity and regulatory developments.

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 • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw