Bird & Bird

Data Protection Monthly Bulletin

September 2022

Welcome to our regular European Data Protection Bulletin

In this edition, we bring you the following updates:

EUROPEAN UNION

EDPB

CJEU

UNITED KINGDOM

ICO

Other UK news

UK Enforcement

ICO Enforcement

Information Tribunal Appeal Cases

EDPB

Date	Description
May	**Draft Guidelines on the calculation of fines under the GDPR** On the 12th May 2022, the EDPB released its draft guidelines on the calculation of fines under the GDPR. These were open for consultation until the 27th June, and we are now awaiting the finalised version. These guidelines are meant to work towards harmonising the process for calculating these fines between the supervisory authorities, including setting consistent starting points for varying levels of severity, and including a list of key factors to consider (whilst leaving scope for supervisory authorities to add more factors, should they consider them relevant).This also clarifies what stage the list of factors specified in Article 83(2) need to be considered, and their impact. The guidelines propose the following sequence of steps: **Identify the relevant infringement(s)** First, the supervisory authority needs to determine which infringement(s) the fine will cover. This is particularly relevant if multiple infringements have been identified, to determine whether multiple fines are warranted. To do this, the supervisory authority is to consider whether multiple infringements constitute one single sanctionable conduct. This could be the case e.g. if they would reasonably be considered by an outside observer to be one coherent conduct, such as the collection and then storage of data. Other examples are where they are legally tied, in particular where one infringement is a specialised version of another (the principle of specialty), a subsidiary part of another (the principle of subsidiarity) or regularly leads to the other- for example by being a preliminary step in the other infringement (the principle of consumption). Finally, they could also be one infringement if a single processing operation breaches multiple GDPR requirements at the same time. Based on these assessments, infringements which constitute a single sanctionable conduct in this way will be assessed together. However infringements that the supervisory authority simply becomes aware of at the same time but are otherwise unconnected are to attract separate fines.

Identify a starting point for the calculation

Supervisory Authorities are then to identify a starting point for the assessment. The EDPB stresses this is simply a starting point, and can be subsequently lowered or raised as is appropriate. This starting point is to be based on:

1. The GDPR categorisation of the infringement (i.e. does it fall under Article 83(4), and therefore have a lower maximum, or Articles 83(5) and (6), and therefore a higher maximum)

GDPR Article	Art. 83(4)	Art. 83(5) and (6)
Fine	€10m or 2% of total worldwide annual turnover	€20m or 4% of total worldwide annual turnover

2. The seriousness of the infringement.
    - This is based on:
        - The nature, gravity and duration of the infringement (Art. 83(2)(a))
          (e.g. to what degree did it infringe on the objective that the GDPR provision sought to protect, how much imbalance is there between the data subject and the controller, how many people were impacted, and how long has the infringement been going on for- including if it infringed the pre-GDPR directive and is still ongoing)
        - Whether the infringement was intentional or negligent (Art. 83(2)(b))
          In this case, intent usually requires both knowledge that the action breached GDPR, and wilfulness to perform this breach. If either of these are not present (e.g. it was just the result of human error) then it will be negligent.
        - Whether Special Category Data or Criminal Conviction data was included in the infringement. (Art. 83(2)(g))
    - The Seriousness is to be classified as “Low”, “Medium” or “High”, and supervisory authorities are to reduce the GDPR maximum fine based on the following ranges to create a new baseline:

Seriousness	Low Seriousness	Medium Seriousness	High Seriousness
Modifier range	0-10%	10-20%	20-100%

3. A further discretionary modification based on the turnover of the company, in order to ensure that the fine is effective, proportionate and dissuasive in all cases. This is in the form of a maximum further multiplier, which is the greatest that the supervisory authority can reduce the baseline down by should they wish to.

Turnover	≤ €2m	≤ €10m	≤ €50m	≤ €100m	≤ €250m	€250m +
Maximum modifier	0.2%	0.4%	2%	10%	20%	50%

For example, a medium seriousness breach of an Art. 83(4) infringement by a company with a turnover of €100m would lead to a supervisory authority deciding a starting point in the following range:

	GDPR Article Fine	Seriousness Modifier	Turnover Modifier	Result
Minimum	€10,000,000	10%	10%	€100,000
Maximum	€10,000,000	20%	None	€2,000,000

Apply Aggravating and Mitigating Circumstances

The remaining Art. 83(2) factors, (c)-(f) and (h)-(j), are to be applied next. The majority of these are only ever aggravating, as factors such as compliance with previously ordered measures or reporting to the supervisory authority are simply factors the GDPR expects of controllers, however measures taken to mitigate the damage to data subjects is a key mitigating factor, along with the breach occurring despite adherence to a code of conduct. Furthermore, the EDPB notes that the degree of responsibility of the controller and cooperation with the supervisory authority may, in exceptional circumstances, constitute mitigating factors if the controller has gone above and beyond what would be expected of them.

The EDPB also provides a brief treatment of the "any other aggravating or mitigating factor" point (Art. 83(2)(k)), giving a timely note that "the onset of a serious pandemic emergency" could be one such mitigating factor. Conversely the EDPB notes that the controller profiting from the breach (e.g. charging a fee for access requests) would be the main aggravating factor under this head.

Effectiveness, Proportionality and Dissuasiveness, and the Cap

Finally, the EDPB notes that the fine must not exceed the statutory cap (and restates the established law on how exactly to establish the relevant worldwide turnover)- but that within that cap there is flexibility for the Supervisory Authority to adapt the fine further based on effectiveness, proportionality, and dissuasiveness (under Art. 83(1)). In particular, the EDPB notes that the Supervisory Authority may elect to be more lenient if the company can definitively prove that they could not pay the fine even after significant restructuring, or that paying the fine would result in its assets losing value to the point of the company not continuing operations (with no possibility of an acquisition by another company), or that the company is suffering due to a their sector going through a particular crisis. However this is only an option available to the Supervisory Authority, and the EDPB quotes the General Court that an obligation to give a discount, e.g. due to a company being unable to afford the fine, would be "tantamount to giving an unjustified competitive advantage to undertakings least well adapted to the market conditions".

Comment

These new guidelines to still leave much up to the discretion of the supervisory authority (in particular the application of mitigating and aggravating circumstances), however this is a welcome step in adding more uncertainty to a previously very variable process. Furthermore, the setting of the baseline for low and medium infringements both at no more than 20% of the GDPR maximum should provide a better measure of the risk in many cases, compared to the very high statutory maximums.

12 May

Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

On 12 May 2022, the EDPB issued new guidance to lawmakers and Law Enforcement Authorities (LEAs) on the implementation and use of Facial Recognition Technology (FRT) in accordance with data privacy legislation. The guidelines may also be useful to individuals interested in data subjects' rights. The main document presents the technology and applicable law and is summarised chronologically in this article.

Three annexes are attached to the Guidelines with practical guidance for FRT projects; Annex I features a template for classifying the extent to which an FRT project might interfere with fundamental rights, and Annex II gives guidance on managing FRT projects in LEAs. In Annex III, the EDPB permits the use of FRT in certain circumstances, such as child abduction cases and automated border control systems.

The EDPB calls for a prohibition on the use of FRT in certain cases:

- remote biometric identification of individuals in publicly accessible spaces;

- facial recognition systems that categorize individuals on the basis of their biometric data into groups regarding their ethnicity, gender, political or sexual orientation or other grounds of discrimination;

- facial recognition or similar technologies that allow the inference of a natural person's emotions;

- processing of personal data in a law enforcement context that would rely on a database populated by the collection of personal data on a large scale and in an indiscriminate manner, for example by collecting photographs and facial images that are accessible online.

What is FRT?

FRT is a probabilistic technology capable of automatically recognising individuals for identification and authentication purposes. It uses components of AI and machine learning to process biometric data, including special categories of personal data. Biometric data is irrevocably linked to a person's identity. As FRT requires the processing of thousands of personal data sets, slight effects of algorithmic discrimination or misidentification could severely affect the rights of individuals and minority groups. FRT is a two-step process requiring an image of a face (the biometric 'sample') from which digital representation of distinct characteristics is extracted (the 'template'). This process is explored further in the Guidelines.

The key functions of FRT are the authentication (also known as 1-to-1 verification) and identification of natural persons. Several hypothetical applications are explored by the EDPB to illustrate the context in which FRT is currently being debated and implemented. These can be found in the Guidelines (page 9), however, should not be considered as part of any preliminary assessment of compliance with the EDDPB's stance on data protection.

Whilst the EDPB recognises the need for LEAs to benefit from the best possible tools, it notes how FRT interferes with Article 8 of the EU Charter of Fundamental Rights (the 'Charter'); a key prerequisite to guarantee other fundamental rights. The EDPB views FRT in the context of law enforcement as part of the solution, but by no means a 'silver bullet'.

The Risks

- Risks are inherent to biometric data due to the data subject's inability to change his or her unique characteristics.
- FRT has an increased risk of being hidden as it is a software functionality and is therefore capable of being integrated into already existing infrastructure (cameras, image databases).
- FRT raises several accuracy concerns around its authentication and identification ability, along with issues around the quality and accuracy of any 'source data' or results. Ex post use is no safer, posing its own specific risks to be assessed on a case-by-case basis (See examples in Annex III). Accuracy must be considered as criteria when assessing compliance, with the EDPB stressing the need for controllers to undertake regular and systematic evaluation of algorithmic processing

The law

The Charter

The EDPB emphasises Articles 7 and 8 when considering the processing of biometric data in an LEA context. As FRT may impact the way in which people feel free to act, it is likely to impact a range of other fundamental rights (see Articles 1, 10, 11 and 12 of the Charter).

The processing of biometric data under all circumstances constitutes a serious interference, regardless of the outcome or any deletion of the biometric template. This interference may stem from an act of law or an act of a public authority. Any legislative measure serving as a legal basis for the processing of personal data directly interferes with Articles 7 and 8 of the EU Charter. The use of biometric data and FRT will also impact Article 1.

The EDPB gives guidance on how FRT might be implemented in accordance with Article 52(1):

- Different applications of FRT will likely require dedicated law on legal basis describing the application and conditions as the processing of biometric data via FRT constitutes a special category of data listed in Article 10 LED.
- The EDPB lists potential indicators that the essence of Articles 7 & 8 rights might be being infringed, for example requirements that online public communication service providers retain, generally and indiscriminately, personal data relating to those services.
- The EDPB gives particular attention to necessity and proportionality
    - Legislative measures should differentiate, and target persons covered by considering the relevant objective, such as fighting serious crime. If all persons are covered in a general manner and without such differentiation any interference with rights will be intensified.
    - Data protection safeguards are required especially where personal data is subject to automatic processing and where there is a significant risk of unlawful access.
    - Processors ought not to have regard to purely economic considerations when determining the level of data security.
    - Different categories of data must be made distinct. This will be based on the potential usefulness of the data for the purposes of the objective pursued.
    - In the interests of foreseeability, laws need to be sufficiently clear in terms to give individuals adequate indicators to the circumstances and conditions on which LEAs can use FRT.

The LED

The LED contains a framework for processing special categories of data via FRT. The Guidelines explore this in the context of LEAs. It is made clear that a mere transposition of Clause 10 LED cannot be invoked as a legal basis for the processing of biometric data via FRT for LEAs, as it would lack precision and foreseeability.

The EDPB outlines when processing might be regarded as 'strictly necessary' and 'manifestly made public'. For example, the fact that a data subject did not set privacy features on a social network is not sufficient to consider that data as manifestly made public.

In the context of automated individual decision-making, including profiling, the EDPB draws attention to the general prohibition at Article 11 LED. As FRT relies on special categories of data, any exemption to this will be subject to a higher threshold and suitable safeguards on data subject rights and freedoms will be required. Article 11(3) prohibiting profiling that results in discrimination based on special categories of personal data must also be considered.

Article 6 LED emphasises the need to distinguish between different categories of data subjects. The EDPB infers that as a rule, the processing of personal data must meet the criteria of necessity and proportionality when categorising data subjects. The distinction between different categories of data subjects appears as an essential requirement when it comes to personal data processing via FRT.

Rights of the data subject

The EDPB states that all data subject's rights as listed in Chapter III of the LED will apply to personal data processing via FRT. Controllers must carefully consider how to (or if they can) meet the requirements of the LED before any FRT processing is launched. Analysis should be given to the identity of the data subjects, how they will be informed and how they might exercise their rights.

The guidance gives advice on further rights in greater detail, such as; rights to erasure , restriction and access. Further, the EDPB suggests additional legal requirements and safeguards including DPIAs, consultations with supervisory authorities, security of processing and logging.

14 June

EDPB Guidelines on certification as a tool for transfer

On 14th June, the EDPB published guidelines for consultation (which closes at the end of September) as to the application of Art. 46 (2) (f) GDPR on transfers of personal data to third countries or to international organisations on the basis of certification. These guidelines are intended to supplement the existing Guidelines (01/2018) on certification and identifying certification criteria in accordance with Arts. 42 and 43 of the GDPR and address specific requirements from Chapter V of the GDPR when certification is relied on as a transfer tool.

The Guidelines clarify that a certification mechanism as a transfer tool must demonstrate the existence of appropriate safeguards provided by the data importer to counter the specific risks of transferring personal data. The object of the certification can be a single processing operation or a set of operations and it will be the data importer who is granted the certification although the responsibility for ensuring that the data processing is compliant remains with the data exporter. As such the data exporter will be obliged to verify whether the certification it intends to rely on is effective in light of the characteristics of the intended processing (i.e. does the certification remain valid and cover the specific transfers in question). The data exporter will also need to check that there is a valid "certification agreement" between the data importer and the certification body and should refer to the certification as a tool for data transfer in the data processing agreement or other data sharing agreement with the data importer.

The data exporter is also required to carry out a transfer risk assessment of the third country's laws and practices in force and depending on the outcome, additional supplementary measures may be needed.

In terms of the certification criteria needed to cover a certification scheme to be used as a tool for data transfers, the EDPB considers that the criteria contained in the Guidelines 01/18, Annex 2 (referenced above) and the Guidance on Certification criteria assessment Addendum already cover the majority of the criteria. However, in order to take account of the CJEU Schrems II ruling, the EDPB considers that the certification should also cover (i) an assessment of the third country legislation; (ii) contractual arrangements between the data exporter and data importer describing the specific transfer to which the certification relates and that third party beneficiary rights are recognised; (iii) rules on onward transfers; (iv) redress and enforcement; (v) process and actions for situations in which national legislation prevents compliance with commitments taken as part of certification; (vi) requirements to notify the data exporter in case of requests for data access by third country authorities and ensuring that the transfers do not result in massive and indiscriminate transfers; and (vii) requirements that ensure that any supplementary measures identified by the data importer are matched by corresponding supplementary measures on the part of the data exporter in order to ensure a fully effective implementation of the importer's supplementary measures.

Finally the Guidelines deal with how to ensure that data importer relying on certification mechanism for data transfers takes binding and enforceable commitments to apply the appropriate safeguards provided by the certification mechanism and state that this would usually be done by way of a contract with the data exporter (such as the existing service agreement or DPA) but that these commitments should be clearly distinguished from any other clauses. The Guidelines contains some recommendations as to what these commitments would need to cover (e.g. the importer commits to comply with the rules specified in the certification intended for transfers and warrants that it has no reason to believe that the laws and practices in the third country, including any requirements to disclose data or authorise access by public authorities, prevent it from fulfilling its commitments under the certification and that it will inform the data exporter of any relevant changes in this regard). The Guidelines also contain an Annex containing examples of supplementary measures to be implemented by the data importer.

CJEU

Date	Description
August	**What is in a name? CJEU gives a wide definition of what constitutes processing of sensitive personal data** On 1st August 2022, the CJEU in Grand Chamber handed down a decision on the scope of Article 9 GDPR. Article 9 defines what constitutes "special categories of personal data", i.e. "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited." Those categories are also referred to as sensitive personal data. In the judgement (C 184/20), the CJEU interpreted "data concerning a natural person's sex life or sexual orientation" very wide, but also raised a few other interesting points. FACTS The case dealt with a conflict of anti-corruption laws in Lithuania and data protection law. The Chief Ethics Commission in Lithuania is tasked with fighting corruption. It asked a director of a public establishment (= the data subject) to declare his and his spouses interests according to the anti-corruption laws. The Lithuanian regime foresaw that certain information from the declaration had to be published on the website of the Chief Ethics Commission, such as the forename and surname and as well income related data. RULING There were two questions before the Court. First, whether the publication obligation violated data protection rules and second, in how far the publication of the name of the spouse constitutes processing of sensitive personal data.

The European Court started its analysis with a proportionality test based on article 52(1) of the Charter of Fundamental Rights, which reads:

"1. Any limitation on the exercise of the rights and freedoms recognised by this charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the union or the need to protect the rights and freedoms of others."

The first parts of the proportionality tests were easily met: the objective of fighting corruption are legitimate interests to start with, and the limitations to the right to privacy were also laid down by law. The more difficult question was whether the publication was necessary to foster the aim of anti-corruption. The CJEU decided that the interests (fighting corruption v. data protection) need to be carefully balanced and depending on the level of corruption in the Member States could be decided differently. In the end, the Court sided with the data subject and found that the Lithuanian legislation did not provide sufficient safeguards against the risk of abuse and as a result such legislation violated the right of the data subject. The Court especially pointed out that the argument of the authority that there were not sufficient resources available to individually check all concerned records was invalid:

"[…] a lack of resources allocated to the public authorities cannot in any event constitute a legitimate ground justifying interference with the fundamental rights guaranteed by the Charter."

In the second part of the judgement, the Court was asked in how far the publication of the name of the spouse constituted processing of sensitive personal data. The Court concluded that already the fact that the gender of the spouse might be "revealed" is enough to constitute processing of sensitive data. An alternative interpretation was available, namely, to interpret the word "concerning" in the text of Article 9 more narrowly. To put it simply: The names Max, Alex or Pat are as such just names, combination of letters. They do not concern sexual orientation, but they reveal in most cultures the gender (more or less as the examples show) and taken in context with the spouse's name, reveal the likely sexual orientation. As a result, the publication of the name of a spouse together with the data subject's name constitutes processing of special categories of personal data, as it indirectly discloses the sexual orientation.

WHAT DOES IT MEAN?

The judgement is in line with previous rulings by the Court to interpret data protection definitions very wide. Overall, it is also a decision that carefully looks at different processing activities; the court stresses that it analyses the publication on the website, not other anti-corruption measures. Looking however at a long line of case law (Lindqvist, Breyer), I feel that we are going into a direction of tightening requirements for controllers bit by bit. After all, many activities concern the processing of personal data, and after this judgement, they are also concerning more and more often the processing of special categories of personal data. This is because a lot of data might, combined with other data, reveal sensitive personal data. Here is an

example: A company might want to post pictures from employees on their intranet. Picture of persons reveal their racial origin, which in turn means that controllers must apply the stricter standard at Article 9 GDPR for justifying the processing. In most cases that means explicit consent. Are we heading towards a form of data protection puritanism?

More recently, on 20 September 2022 the Advocate General of the CJEU gave an Opinion on a referral (in relation to Meta in Case C-252/21) which somewhat curtails the broad view. The Advocate General considered that:

"The decisive factor for the purpose of applying Article 9(1) of the GDPR is, in my view, whether the data processed allow user profiling based on the categories that emerge from the types of sensitive personal data mentioned in that article.

39. In that context, to be able to determine whether data processing falls within the scope of that provision, it might be worth distinguishing, where appropriate, between the processing of data which prima facie may be categorised as sensitive personal data, which alone allow profiling of the data subject, and the processing of data that are not inherently sensitive but require subsequent aggregation in order to draw plausible conclusions for profiling purposes."

It will be interesting to see where the CJEU lands when it makes its final decision in the Meta case and whether this signals a tightening or a loosening of the current judgment.

Information Commissioner's Office (ICO)

Date	Description
14 June	**ICO funding update: Fine income retention agreement** On 14 June 2022, the Information Commissioner's Office released a statement announcing that the Department for Digital, Culture, Media & Sport and the Treasury had agreed that the ICO would now be able to retain some of the funds paid as a result of civil monetary penalties. Previously, income from fines was given to the Government's central Consolidated Fund. Now, up to £7.5m a year can be retained by the ICO. This will be audited by the National Audit Office. The change will assist the ICO in tackling more complicated enforcement litigation. James Dipple Johnstone, Chief Regulatory Officer, said: "Being able to recover some of our litigation costs will form an important part of ensuring that the ICO has the right tools to do our job. We are on the side of the public and responsible businesses and being well resourced to take action can give everyone the confidence that, where appropriate, we will act effectively to uphold rights."
30 June	**ICO sets out revised approach to public sector enforcement** On 30 June 2022, the Information Commissioner's Office set out a revised approach to working more effectively with public authorities. The approach, set out in an open letter from the Information Commissioner, expressed an intention to be more collaborative with the public sector, and to work towards deterrence and prevention over fines.

	Specifically, the Commissioner will seek better engagement with public sector bodies to prevent breaches and harm before it occurs. This will include use of the ICO's wider powers, including warnings, reprimands and enforcement notices. The ICO has said it will take a discretionary approach to imposing fines and will usually reserve them for particularly serious cases. Where fines are imposed, the ICO will also promote greater transparency. When a fine is considered, the decision notice will give an indication on the amount of the fine the case would have attracted. This can act as a deterrent and provide wider market signals to public entities. The ICO also has a commitment from the UK Government, to create a cross-Whitehall senior leadership group to encourage compliance with high data protection standards.
5 July	**UK's agreement in principle to an adequacy decision with South Korea** On 5 July 2022, the UK and South Korea signed a **Data Adequacy Agreement in Principle.** This is the first 'in principle' adequacy decision the UK has entered post-Brexit. As an adequacy decision, this document demonstrates that each country is comfortable with the level of protection of personal data provided by the other. The European Commission also granted an adequacy decision to South Korea in December 2021. The decision, when finalised, will enable the transfer of data between countries without the need for contractual protections. The agreement will enable UK businesses to operate more seamlessly with partners in South Korea and to reduce administrative and financial compliance costs companies would normally face when transferring data overseas. Alongside the Data Adequacy Agreement, the UK and South Korea have also signed a Memorandum of Understanding (MoU). In it, the ICO and the South Korean Personal Information Protection Commission have agreed to co-operate on specific projects, share experiences and best practices, and intelligence to support their regulatory work.
8 July	**ICO and NCSC advice against making ransomware payments & new guidance against the threat of credential stuffing attacks** On 8 July 2022, The Information Commissioner's Office ("ICO") and the National Cyber Security Centre ("NCSC") released a joint letter requesting the Law Society remind members of the profession about their obligations and the appropriate response to a ransomware attack.

In particular, the joint letter reiterated pre-existing advice that members should not pay ransomware demands. It noted in particular that ransomware payments were at risk of breach of sanctions (particularly those related to Russia) and that those who pay them may face penalties. There is also a danger that ransomware payments fund further harmful behaviour by cyber attackers and do not guarantee decryption of networks or return of stolen data.

When an attack has occurred, the letter sets out the appropriate response to a ransomware attack. For a full overview of the steps, see the full guidance. There is a regulatory requirement to report to ICO as the data regulator where there is a breach. Determining if there is a requirement to report can be assisted by the ICO's self-assessment portal. In addition to the ICO's support, NCSC can provide support and incident response to mitigate harm and learn broader cyber security lessons. The NCSC has a ransomware hub which sets out its guidance in one place.

Other UK News

Date	Description
Consultation response: June 2022	**UK Data Reform: Government publishes data protection reform consultation response and draft bill**
Draft bill: July 2022	Following Brexit, the Government promised that the UK's data protection regime would be reformed as part of its National Data Strategy. The Government has now followed through and published both (i) a response to its original consultation "**Data: A New Direction**" (first launched in September 2021) on 23 June 2022 (the "response"); and (ii) a draft **Data Protection and Digital Information Bill** on 18 July 2022 (the "bill"). **Consultation response** The response paints the outcome of the consultation as promoting a step forward for both businesses and individuals in terms of, for example, cost savings, innovation, and clarity around privacy rights. The proposals are grouped into five chapters covering (i) reducing barriers to responsible innovation, (ii) reducing burdens on businesses and delivering better outcomes for people, (iii) boosting trade and reducing barriers to data flows, (iv) delivering better public services, and (v) reform of the ICO. The response highlights the key themes amongst submissions by respondents, and sets out both the proposals which the Government has taken forward but also those it has rowed back on. On 16 June 2022, the new Information Commissioner, John Edwards, issued a statement confirming that the ICO supports the Government's proposals and in particular, the fact that the Government had taken concerns about the ICO's independence on board (see Chapter 5 of the response). Note that there will likely still be significant changes to the structure and duties of the ICO (see "Role of the ICO"), below. **Draft bill**

Following on from the response, the draft Data Protection and Digital Information Bill (the "bill") was introduced to Parliament on 18 July 2022 and was forecast to have its second reading on 5 September 2022, but this has been delayed in light of the leadership election and to allow ministers to consider the legislation further.

The bill is structured in 6 parts: Part 1 deals with key changes to the data protection framework; Part 2 regulation of digital verification services; Part 3 smart data schemes; Part 4 other digital information-related changes, including amendments to PECR; Part 5 statutory oversight including the structure of the ICO; and Part 6 consequential revisions, financial provision and commencement.

The key reforms proposed in the response and effected through the bill can be summarised as follows:

- **Accountability** – the new UK GDPR accountability regime will require businesses to implement less prescriptive and more risk-based privacy management programmes. The role of DPO has been replaced with a "senior responsible individual", whose role and tasks are set out in new provisions; and DPIAs are replaced by "assessments of high risk processing". ROPA requirements have been simplified and the UK representative requirement has been removed.
- **Lawful basis** – the bill creates a whitelist of legitimate interests which will always outweigh the interests of individuals (i.e. removing the need to conduct a balancing test), set out at Annex 1 to the UK GDPR and covering disclosures in the context of public interest tasks, national security, emergency response, crime, safeguarding vulnerable individuals, and democratic engagement. The Secretary of State is empowered to amend this list over time.
- **Purpose limitation** – the bill condenses the UK GDPR's previous requirements and guidance around purpose limitation into a single provision for clarity, with the addition of an Annex 2 to the UK GDPR setting out a whitelist of purposes which will automatically clarify as compatible with the original purpose of processing. Annex 2, like Annex 1, can also be updated by the Secretary of State. There is a restriction around further processing of personal data which was originally collected based on consent.
- **Research and development** – the bill has also simplified provisions relating to research and development. Interpretive recital language has been moved into the main text to have greater force. There is a new exemption to providing notices under Article 13, and further clarity on broad consent for research.
- **AI** - The automated decision making provision has been reframed to be a requirement for safeguards to be in place rather than a prohibition with exceptions (it has not, however, been removed in its entirety as had been tabled previously). Separately, the bill gives clarity on permitting the processing of special category data for AI bias monitoring purposes. Further AI developments have been postponed until an upcoming AI Governance White Paper.

- **Anonymisation** – through the insertion of a new provision regarding "information relating to an identifiable living individual" in the DPA 2018, the bill codifies the UK's historically pragmatic approach to anonymisation by clarifying that the assessment of identifiability is only required to be made from the perspective of the relevant controller or processor, or another person who the controller or processor ought to know will or is likely to obtain the information as a result of the processing (by contrast to the assessment from the perspective of "anyone in the world" required by stricter regulators).
- **DSARs** - the threshold for refusing DSARs has been changed from "manifestly unfounded or excessive" to "vexatious or excessive" to expressly align with the FOIA exemption. A new provision suggests possible interpretations of this phrase in line with existing ICO guidance (for example, requests intended to cause distress, not made in good faith, or an abuse of process).
- **International transfers** – the proposal to allow exporters to determine their own safeguards has been dropped, but the bill reflects the Government's promised more "commercial" approach to assessment of adequacy and transfer risks. The bill creates a "data protection test" for the Secretary of State and exporters to use when assessing adequacy/transfers, and specifies that exporters must make the assessment "acting reasonably and proportionately" determined by reference to the circumstances. The international transfers provisions are likely to come under particular scrutiny when considering whether the UK's adequacy decision from the EU is at risk.
- **Direct marketing** – the bill extends the remit of the "soft-opt-in" in PECR to cover email marketing "solely for the purpose of furthering a charitable, political or other non-commercial objective" subject to similar safeguards to the existing provision, with the aim of benefitting charities and political parties. The ICO will have increased powers around nuisance calls and will be able to consider the calls made by controllers as well as those received by individuals.
- **Adtech and cookies** - there was significant publicity in the run-up to the bill around abolishing of "cookie banners" in favour of an opt-out browser model. The bill permits the Secretary of State to issue regulations to permit this approach but this would only in respect of websites not likely to be accessed by children, and once the appropriate technology is available (which could take some time). In the meantime the bill also amends PECR to allow businesses to place more cookies without opt-in consent for "non-intrusive" purposes which include certain analytics purposes.
- **Enforcement** – the bill increases fines for breach of PECR up to GDPR levels, i.e. the higher of £17.5 million or 4% of the total worldwide annual turnover in the preceding financial year. The bill gives the ICO certain additional powers in investigations, though places other responsibilities around responding to initial complaints from data subjects back on the controller.
- **Role of the ICO** – the bill makes expansive changes to the ICO's structure, strategy and oversight. It will be replaced by a corporate body, the "Information Commission". Significantly, it will be required to consider the promotion of economic growth and impact on competition, and the Secretary of State must approve

statutory guidance before it is laid before Parliament, which could lead to a more pragmatic overall approach.

The Government has also released the following materials in conjunction with the bill:

- Explanatory notes to explain the purpose of the bill;
- A Delegated Powers Memorandum to justify any delegations of powers (e.g. to ministers) in the bill;
- Impact assessments here and here; and
- A House of Commons Library Research Briefing, aimed at presenting a politically impartial summary of factual information and opinions on the bill.

The next steps for the bill are to proceed to the delayed second Parliamentary reading and further subsequent stages in Parliament, before going through readings in the House of Lords and finally receiving Royal Assent.

This Data Protection Bulletin will stay abreast of further updates to the bill. You can also read Bird & Bird's opinion pieces on the response here and here.

UK ICO Enforcement

Date	Entity	Type of Breach & Sanction	Description of Breach
26 May	Clearview AI Inc.	GDPR (Article 5, 6, 7, 14, 15, 16, 17, 21, 22 and 35) Monetary Penalty of £7,500,000 Enforcement Notice	The ICO issued a £7.5million fine against Clearview AI Inc ("Clearview") for its continued infringement of the UK GDPR, finding that the company: failed to have a lawful reason for collecting people's information; did not have a process in place to stop the data being retained indefinitely; and failed to use the information collected in a "fair and transparent" way. This fine is significantly reduced from the original £17 million proposed in the ICO's November 2021 provisional notice. The ICO also issued an enforcement notice ordering Clearview to "stop obtaining and using the personal data of UK residents that is publicly available on the internet, and to delete the data of UK residents from its systems". The ICO's decision follows a joint investigation with the Office of the Australian Information Commissioner, and the UK is now the fourth country to have fined Clearview alongside Italy, France and Australia. Clearview, an American business, operates an algorithmic image search which allows customers to match a "Probe image" against Clearview's database of images, metadata and URLs. Clearview's database has been grown from the public-facing internet (including Facebook, Instagram and other platforms) without gaining permission from individuals. It currently stores more than "20 billion faces". Given the high number of UK internet and social media users, the Commissioner considered that the database is likely to include a significant amount of data from UK residents, gathered without their consent. Furthermore, despite no longer offering its services to UK organisations, Clearview was previously trialled by 5 different UK law enforcement agencies, including the Metropolitan Police, to assist with criminal prosecutions. Clearview also continues to have customers in other countries who can use and access the personal data of UK residents. Therefore, the Commissioner determined that there remains a "clear potential for both damage and distress to be

			suffered by data subjects when their images are matched with a Probe Image, especially if the match turns out to be inaccurate and erroneous." The ICO found the Clearview had breached UK data protection laws on the following grounds: • failing to use the information of people in the UK in a way that is fair and transparent, given that individuals are not made aware or would not reasonably expect their personal data to be used in this way; • failing to have a lawful reason for collecting people's information; • failing to have a process in place to stop the data being retained indefinitely; • failing to meet the higher data protection standards required for biometric data (classed as 'special category data'); and • asking for additional personal information, including photos, when asked by members of the public if they are on their database. This may have acted as a disincentive to individuals who wish to object to their data being collected and used. The Commissioner also considered whether it was practicable for Clearview to comply with the enforcement notice, however it concluded that Clearview would be able to: • within 6 months, delete any personal data of data subject's resident in the UK held on their database, and other data associated with such images; and • within 3 months of the expiry of the appeal, refrain from processing any further personal data of subject's resident in the UK. Clearview has appealed the ICO's decisions and is not required to comply with the enforcement notice or pay the fine until the appeal is determined.
30 June	The Tavistock & Portman NHS Foundation Trust	GDPR (Articles 5(1)(f), and 32(1) & (2))	The ICO issued a £78,400 fine against The Tavistock & Portman NHS Foundation Trust ("the Trust") following emails sent to 1,781 Gender Identity Clinic ("GIC") patients which did not use the Blind Carbon Copy (BCC) feature. The Trust's GIC accepts UK wide referrals for patients who experience difficulties in the development of their gender identity. In 2019, the Trust became involved in the

		Monetary Penalty of £78,400	promotion of an art competition aimed at engaging its GIC's patients in the clinic's refurbishment. The Trust intended to send a bulk email to the GIC's active patients who had consented to being contacted by email in certain circumstances in relation to the art competition. On 6 September 2019, the promotion email advertising the art competition and welcoming submissions from the Trust's GIC patients was sent. However, in error, the email addresses were copied into the "To" field, instead of the "BCC" field. This meant the recipient receiving the email could see all the other recipients in copy. There was an immediate attempt to recall the emails which was unsuccessful. The Trust (on the same day) emailed the affected data subjects regarding the breach, posted a notification message on the Trust's website, and formally notified the ICO. The Commissioner considered that despite the Trust having some measures in place to secure the data of its patients, they were insufficient given the "particular sensitivities around the nature of the personal data" and the Trust had failed to take the necessary steps as a data controller and processor to secure the processing of data. Further, the ICO found the infringements amounted to a serious failure to comply with the GDPR and noted the Trust experiencing two similar incidents in 2017. Following the ICO's new approach to public sector enforcement (which will see the Commissioner trialling discretion to reduce the impact of fines on the public sector over two years) the fine was reduced from £784,800 on the basis the Trust had taken prompt action following the breach.
3 August	Christopher O'Brien	Data Protection Act 2018 (Section 170) Compensation to each data subject of £250	Christopher O'Brien, a former Health Advisor, was prosecuted for accessing the medial records (i.e., obtaining the personal data) of 14 patients of South Warwickshire NHS Foundation Trust, each of whom he knew personally. He obtained the records during his employment, without business need to do so and had not obtained the consent of his employer. He was ordered to pay compensation of £250 to each data subject totalling £3000. ICO Director of Investigations, Stephen Eckersley, said that the case serves as a reminder that "just because your job may give you access to other people's personal

	information, especially sensitive data such as health records, that doesn't mean you have the legal right to look at it."

Information Tribunal Appeal Cases

Date	Appellant	Type of Case and Result	Summary of Case
1 June 2022	Olufunke Osifeso	Application for an appeal against a Tribunal decision given in connection with s166 DPA 2018. Dismissed	On 1 July 2019, and then again on 9 December 2019, Ms Osifeso made complaints to the ICO about how the Royal Bank of Scotland (RBS) had handled her personal data. Dissatisfied with the response, she then applied to the General Regulatory Chamber (GRC) of the First-tier Tribunal under section 166 of the Data Protection Act (DPA) 2018. On 31 January 2020 a GRC registrar struck out Ms Osifeso's application on the basis that it had no reasonable prospect of success. Ms Osifeso applied for the matter to be considered afresh by a Judge, and on 20 February 2020 Judge Macmillan carried out that reconsideration but reaffirmed the strike out ruling imposed by the GRC registrar. She also refused permission to appeal to the Upper Tribunal on 30 March 2020. Ms Osifeso then applied to the Upper Tribunal for permission to appeal, which was granted on 24 August 2020. Ms Osifeso's further appeal was subsequently stayed pending the outcome Killock and Veale v Information Commissioner [2021] UKUT 299 (AAC).

On paper, the applicant argued there was a procedural issue relating to what the appropriate steps might have been for the ICO to take in investigating her complaint – in effect that the ICO had failed to take appropriate steps to respond to her complaint (DPA 2018, section 166(1)(a)) by failing to investigate the subject matter of her complaint to the extent appropriate (DPA 2018, section 165(5)). She denied that she was challenging the Commissioner's substantive response to her complaint.

As such she asked the Upper Tribunal to reconsider the decision made by the First Tier-Tribunal, which had rejected her application for the lower court to analyse the procedural steps the ICO took when investigating her complaint.

The Upper Tribunal dismissed the appeal against alleged procedural problems with a decision made by the ICO in relation to a complaint.

Other recent articles

- **Making Privacy Paramount - Anna Morgan, a partner in Bird & Bird's new Dublin office, discusses children's privacy online with Oran Kiazim, the Vice President of Privacy at Paramount.**
- **Latest updates in the APD v IAB Europe case in Belgium**
- **Restraining disclosure of overheard private, business conversations – Eavesdroppers beware!**
- **Evolution of the automotive sector – data privacy and cyber security**
- **UK data protection reform: winners, losers and what to watch**

Previous and upcoming events

- **Data, Drugs & Devices: Decoding Digital Health event in Brussels**
- **With the EU NIS2 Directive come stronger cybersecurity measures: Next steps for companies**
- **Dark Patterns, Data Protection and Design Webinar**

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

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority (SRA) with SRA ID497264. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.