RPC

COMMERCIAL LAW

# Snapshots

SPRING 2021

KEY DEVELOPMENTS FOR TODAY'S COMMERCIAL LAWYER

# Your **data** fix

# European Data Protection Board (EDPB) issues draft guidelines for data breach notification

### The question

What more could be done to aid data controllers in responding to personal data breaches and the practical considerations they face while operating under the General Data Protection Regulation (GDPR)?

### Key takeaway

The EDPB "Guidelines 01/2021 on Examples regarding Data Breach Notification" (Draft Guidelines) are intended to be used by data controllers in conjunction with their pre-existing tool kit to effectively manage and prevent data protection breaches. These new Draft Guidelines are not intended to serve as a comprehensive list of recommended actions, as every incident requires its own assessment and appropriate actions.

### The background

The EDPB accepted that the guidelines on personal data breach, produced by the former EDPB Article 29 Working Party, lacked adequate detail and provided little by way of practical considerations. In response, the EDPB has published its Draft Guidelines to provide data controllers new guidance on how to better handle prevent, understand and respond to data breaches.

### The guidance

The Draft Guidelines outline six categories of data breaches with example cases as listed below. Many of these examples refer to "data exfiltration", which essentially means a form of security breach (often using malware) when an individual or company's data is copied, transferred or retrieved from a computer or server without authorisation.

1. **Ransomware**
   - Ransomware with proper backup and without exfiltration (Case No.01)
   - Ransomware without proper backup (Case No.02)
   - Ransomware with backup and without exfiltration in a hospital (Case No.03)
   - Ransomware without backup and with exfiltration (Case No.04)

2. **Data exfiltration attack**
   - Exfiltration of job application data from a website (Case No.05)
   - Exfiltration of hashed password from a website (Case No.06)
   - Credential stuffing attack on a banking website (Case No.07)

3. **Internal human risk**
   - Exfiltration of business data by a former employee (Case No.08)
   - Accidental transmission of data to a trusted third party (Case No.09)

4. **Lost or stolen devices or paper documents**
   - Stolen material storing encrypted personal data (Case No.10)
   - Stolen material storing non-encrypted personal data (Case No.11)
   - Stolen paper files with sensitive data (Case No.12)

5. **Mispostal**
   - Snail mail mistake – sending of incorrect packing bills with goods to customers (Case No.13)
   - Sensitive personal data sent by mail by mistake (Case No.14)
   - Personal data sent by mail by mistake (Case No.15)
   - Snail mail mistake – sending of two different insurance summaries to one recipient (Case No. 16)

6. **Social engineering**
   - Identity theft (Case No.17)
   - Email exfiltration (Case No.18)

The example cases within the categories highlight the practice-based focus of the Draft Guidelines and further serves to provide data controllers with a wide-ranging list of forms data breaches can take.

Each case in the Draft Guidelines is broken down into two sections:

A. **Prior measures and risk assessment** – this section looks at reducing the overall likelihood of data breaches occurring whilst providing guidance on how to assess the risks from a breach. It cites examples such as implementing proper patch management, the use of appropriate anti-malware detection systems, proper and separate backup systems and providing employee training (SETA program).

B. **Mitigation and obligations** – this section is concerned with mitigating the damage caused by the data breach and the resultant obligations on the data controller. It suggests carrying out an impact assessment, ensuring there is an incident response process, documenting all data breaches in accordance with Article 33(5) and knowing when an obligation to communicate with the data subject arises.

### Why is this important?

The previous EDPB guidelines were more theoretical than practical, and the practice-based, example-driven approach of the new Draft Guidelines should be welcomed. They provide greater clarity and concrete guidance for both the prevention and mitigation of data breaches.





### Any practical tips?

The UK is of course no longer a member of the EU, but the GDPR remains at the core of data protection law in the UK and, although the ICO has final authority on these issues, it is highly unlikely the ICO will deviate from the EDPB's Draft Guidelines. Either way, the categorisation and recommendations in the Draft Guidelines should certainly be welcomed by data controllers in the UK.

The Draft Guidelines emphasise good practice in lieu of strict legal obligations and aims to provide accountability to data controllers. Remember that the categories and examples provided are not intended to be used as an exhaustive list. It goes without saying that data protection is one of the fastest evolving areas and no single list can accurately depict all forms of data breaches.

# ICO resumes investigation into real time bidding (RTB) and AdTech

### The question

What will be the ultimate impact of the ICO's continuing investigations into RTB and AdTech?

### Key takeaway

In May 2020 the ICO paused its investigation into RTB and the AdTech industry, since they prioritised activities responding to the COVID-19 pandemic. The ICO has now resumed the investigation into RTB and data processing. The ICO has said that the complex system of RTB uses people's sensitive personal data to serve ads requires explicit consent, which is currently not happening.

### The background

Having started its review into RTB in February 2019, the ICO paused its investigation into the matter following the start of the pandemic. With things beginning to settle down, the ICO has now been able to resume its investigation.

In a statement in early 2020, the ICO highlighted a lack of transparency due to the nature of the supply chain and the role different actors play in RTB. Six months were given to the RTB industry to work on the points raised by the ICO, which ended in May 2020, when they paused the investigation. The key concerns at the time were, among others:

- the use of "legitimate interests" as the lawful basis for the processing of personal data in RTB being insufficient
- the lawfulness of processing of special category data and the processing of non-special category data without consent
- the reliance on contracts for data sharing across the supply chain
- the lack of transparency on what happens with users' data
- wider security and data sharing issues caused by this data supply chain.

### The development

The ICO has announced that its investigation will continue with a series of audits focusing on data management platforms. They will also be issuing assessment notices to specific companies in the coming months where necessary. Naturally, the ICO will be publishing their final findings at the conclusion of the investigation.

### Why is this important?

The sharing of data with potentially hundreds of companies, without properly assessing and addressing the risk of these counterparties, raises huge questions from a data compliance perspective, including around the security and retention of this data.

Since the ICO is committed to undertaking further investigations and assessments as to the processing of data for RTB, organisations should be reviewing their practices urgently with a view to avoiding any possible action by the ICO.

### Any practical tips?

All organisations operating in the RTB space should assess how they use personal data as a matter of urgency. It's no easy task, but any review should focus on users' consent, legitimate interests, data protection by design and any data protection impact assessments, including through their supply chain. The ICO's guidance should be kept front of mind. Data compliance and RTB is an issue that is not going away.





# DCMS publishes prototype trust framework on digital identity products and services

### The question

What is the potential impact of the trust framework on the provision and use of digital identity services published by the Department for Digital, Culture, Media & Sport (DCMS)?

### Key takeaway

The draft "alpha" framework sets out principles, policies, procedures and standards governing the use of digital identity to allow for the sharing of information to check people's identities or personal details. It also sets out the requirements that organisations will have to meet in order to be certified against the framework once, as is expected, it becomes law.

### The draft framework

The publication of the draft framework follows off the back of the call of evidence on digital identify policy in July 2019. It sets out specific future standards and requirements for organisations which provide or use digital identity services, including:

- how organisations should handle and protect people's data (published through a data management policy)
- what security and encryption standards should be followed
- informing users of changes made to their digital identity and how their accounts are managed
- having account recovery processes and notifying users if organisations suspect a user's account has been fraudulently accessed
- following guidance on how to choose secure authenticators for their service.

Under the new framework organisations will also have to publish a yearly report explaining which demographics have been, or are likely to have been, excluded from their service and why. Additionally, the framework promotes "vouching" where trusted people within the community such as doctors or teachers "vouch for" or confirm a person's identity as an alternative to using traditional identification documents (eg passports and driving licences).

### Why is this important?

All organisations providing or using digital identity services will need to meet the requirements in order to be certified against the trust framework. It is therefore important to start preparing ahead of the framework becoming law in the future in order to ensure compliance ahead of certification.

### Any practical tips?

The deadline for any comments from organisations was 11 March 2021 through an electronic survey. Following comments, the DCMS will incorporate the feedback into the framework and intends to publish a second iteration in short order after March 2021 containing further details relating to the framework and certification.

The publication of the "alpha" framework allows organisations to start planning ahead of the implementation of the framework into law and the introduction of any new requirements. If you're providing digital identity products and services, now is the time to start studying how the framework may impact your business. Equally, if you rely on third party providers of these services, consider how to start integrating the requirements into your contracts.

# ICO launches data analytics toolkit

### The question

What's in the ICO's new data analytics toolkit, and how far down the privacy compliance road does it take you?

### Key takeaway

The UK Information Commissioner's Office's (ICO) new toolkit provides organisations with key data protection points they need to consider for any project which involves data analytics and personal data.

### The background

As part of its priority work on artificial intelligence (AI), the ICO has launched a new toolkit for organisations which are planning to use personal data for data analytics. The toolkit outlines important personal data protection considerations which organisations should consider at the beginning of any scheme involving personal data processing. It is part of the ICO's AI priority work and follows the ICO's recent publications "*Explaining decisions made with AI*" and "*Guidance on AI and data protection*". As the ICO notes, the toolkit will assist businesses in identifying some of the most significant risks for individuals' privacy rights and freedoms that can result from the use of personal data analytics. The ICO stresses that many data analytics risks are context specific, so the toolkit cannot guarantee complete compliance with data protection law. That said, it should be regarded as one of your main starting points on any data analytics project you are considering.

### The toolkit

The toolkit is aimed at assisting organisations at the beginning of a data analytics project lifecycle. It focuses on helping recognise some of the central risks to the rights and freedoms of individuals created by the use of data analytics and is designed to be a basic introduction to some of the risks to individuals that data analytics may create or worsen.

Many of the risks that arise from the application of data analytics are context specific, therefore the ICO cannot include an exhaustive or definitive list of issues to consider. Naturally assessing the risk in the context of organisations processing activities form part of the organisation's responsibility as a controller. The toolkit therefore comes with the clear caveat that: "*you should not view this toolkit as a pathway to absolute compliance with data protection law, but as a starting point for what you will need to consider*".

The toolkit is designed for organisations and their data protection officers (DPOs) to consider risks, rights and freedoms in the context of data protection law. It is not a comprehensive analysis of every factor that needs to be considered when implementing a data analytics system. Although there are links between the fairness principle of data protection law to ethics and equality, organisations will need to consider these and other elements separately to ensure they are compliant with any additional obligations they may have.





### Data analytics

The toolkit defines data analytics as "*the use of software to automatically discover patterns in data sets (where those data sets contain personal data) and use them to make predictions, classifications or risk scores*". Integral to data analytics as defined by the ICO are algorithms, and organisations are increasingly using a specific category of advanced algorithm, namely AI to complete tasks. The ICO defines AI as "*the theory and development of computer systems able to perform tasks normally requiring human intelligence*" and cross-refers to the ICO's earlier guidance on AI for an analysis of the risks that the use of AI can create for individuals. The ICO stresses that the toolkit can assist regardless of whether AI is used in connection with personal data analytics projects.

### How does the toolkit work?

The toolkit starts by asking various questions to determine the legal regime the organisation will be processing under as well as questions relating to lawfulness, accountability and governance, the data protection principles, and data subject rights. Upon using the toolkit, a short, tailored report is created suggesting practical actions the organisation can take and provides links to additional guidance that will help the organisation improve its data protection compliance. The ICO notes that complying with these recommendations is not a guarantee that the toolkit will comply with data protection law, and it is crucial that organisations consider the advice the ICO gives in the context of processing and seek the advice of their DPO where needed.

The ICO further notes the toolkit is anonymous, and the answers provided are not visible to or retained by the ICO. It advises organisations to download a copy of the report generated and retain this for future reference.

### Why is this important?

It is vital that data protection compliance is built in from the start whenever data analytics are being contemplated to process personal data. This is not only the law but a crucial step in gaining public trust and confidence.

The toolkit is a useful practical addition to the ICO's two pieces of guidance on AI referred to above, namely "*Explaining decisions made with AI*" and "*Guidance on AI and data protection*". Although none of these, either individually or combined is intended to provide a one-size fits all solution, they do provide a strong foundation for data protection compliance and their application will provide key evidence of accountability under the GDPR.

### Any practical tips?

The toolkit is a welcome addition to compliance processes when commissioning, designing, and implementing data analytics. It's definitely a good place to start on any of these projects, but there's no substitute for doing a deeper dive with your DPO. After all, data compliance sits at the heart of any analytics programme and getting the privacy building blocks lined up correctly from the start is crucial.

Global Expertise.
Local Connections.
Seamless Service.

TERRALEX

www.terralex.org

Explore the key developments across commercial, data, digital, consumer and advertising law in **Snapshots Spring 2021**.

rpc.co.uk