UKTraining

The GDPR Update

Course book

Course book

This document contains the text of the PowerPoint displays that are used during the presentation of the course

The GDPR Update

UK Training (Worldwide) Limited
17 Duke Street
Formby
L37 4AN

Website: www.uktraining.com
Email: info@uktraining.com
Telephone: 01704 878988

Contents

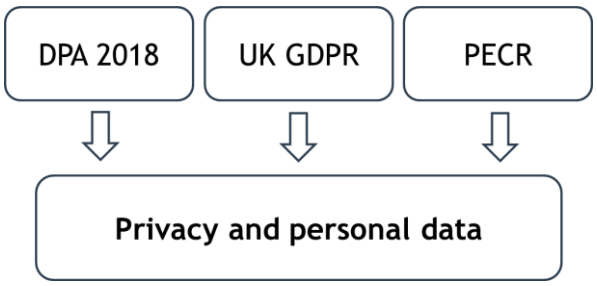
Session 1: The UK data protection landscape

Data protection in the UK after Brexit

- The UK now has the UK GDPR (United Kingdom General Data Protection Regulation)
  - Created by the European Union (Withdrawal) Act 2018
  - Updated by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and 2020 **'EU Exit Regulations'**
- The Data Protection Act 2018 has also been updated
- The Privacy and Electronic Communications Regulations (PECR) remains in place but will refer to the UK GDPR

The UK data protection regime

UK GDPR, DPA 2018 and PECR are applied jointly



Penalties and enforcement under UK GDPR

- For (mainly) a breach of record keeping, contracting and security clauses
  - Maximum fine of up to **£8.5 million** or **2%** of annual worldwide turnover… whichever is greater
- For (mainly) a breach of the basic principles, Data Subject Rights, transfer to third countries, non-compliance with an EU DPA order
  - Maximum fine of up to **£17 million** or **4%** of annual worldwide turnover… whichever is greater

Dual regime

- The UK GDPR has extra-territorial scope
- Some businesses will be subject to both regimes - it is best to assess the application of each regime separately
- Organisations with pan-European operations are likely to have to comply with two separate, but similar, legislative regimes
- Risk of dual enforcement action in the event of any breach
  - EU Data Protection Authorities in the EU and the ICO in the UK
- UK organisations that are subject to EU GDPR but have no establishment within the EU may have to appoint an EU representative and vice versa

Data transfers

- The UK is now a third country for the purposes of the EU GDPR
- On the 28th June 2021 the EU granted adequacy status to the UK allowing the transfer of personal data from EU countries
- For the first time, the adequacy decisions include a so-called ‘sunset clause', which strictly limits their duration to four years
- After that period, the adequacy findings might be renewed, but only if the UK continues to ensure an adequate level of data protection
- During the 4 years, the Commission will continue to monitor the legal situation in the UK and could intervene at any point

- The UK GDPR automatically recognises all EU countries as adequate and recognises all existing EU adequacy decisions
- Transfers from the UK to other countries can continue under existing arrangements
- Check that your privacy notices and other documentation (contracts and records of processing) reflect these transfers appropriately

The future of data protection in the UK…

- The Government launched a consultation on UK data protection reform containing a number of proposals:
  - Likely changes to both UK GDPR and the UK PECR
  - Probable relaxation of several areas of UK GDPR, with a focus on outcomes rather than prescribed processes
  - Plans to increase fines under PECR to match those under GDPR - a clear warning to anyone disregarding marketing rules
- Overall aim to drive economic growth and innovation and strengthen public trust in use of data
- Government clearly hopes any changes will enable the UK to retain adequacy status

Proposed changes

- Changes to the **accountability** framework, with businesses expected to have **a Privacy Management Programme (PMP)** in place
- Removal of the mandatory requirement to appoint a **DPO**
- No mandatory requirement for **Data Protection Impact Assessments**
- More **flexible record keeping** proposed to replace RoPA (Records of Processing Activities)
- **Data breach notification** threshold changes to reduce over-reporting
- Data **Subject Access Requests** changes

Proposed changes

- Changes to **cookies**, with 2 options proposed…
  - Use of cookies without the consent - treated the same as 'strictly necessary' cookies
  - Store or collect information from a user's device without their consent for other limited purposes
- Proposal to create an exhaustive list of **legitimate interests**, i.e. no Legitimate Interest Assessment (LIA) required
- Extended use of the PECR's '**soft opt-in**'
- Reform of the **ICO**

ICO response to the consultation

- Cookies
  - Supports removal of the requirement to obtain consent for analytics cookies,
  - Suggests appropriate safeguards should be retained
- Direct marketing
  - Supports proposal to increase fines imposed under PECR to match UK GDPR
- ICO reforms
  - Highlights a key concern - identifies that the power of the Secretary of State to approve or reject codes of practice may represent a challenge to the ICO's independence

ICO consultation on international transfers

- On 11th August 2021, the ICO launched a consultation on its draft international data transfer agreement (IDTA) and guidance for organisations on international transfers
- Once finalised, the IDTA will replace the existing EU Standard Contractual Clauses (SCCs) in the UK
- The ICO's consultation is split into three sections:
  - Proposal and plans for the ICO to update its guidance on international transfers
  - Transfer risk assessments
  - ICO model international data transfer agreements

International Data Transfer Agreement (IDTA)

- The draft IDTA is intended to provide UK-specific standard contractual clauses for transfers of personal data to third countries - *ico.org.uk/media/about-the-ico/consultations/2620396/intl-data-transfer-agreement-202100804.pdf*
- It consolidates the full range of SCCs that may be required into a single agreement
- Other features to note are:
  - Tables to help with setting out specific information about the exporter, importer, and the purposes of the restricted transfer
  - to exclude extra protection clauses
  - Option to include commercial clauses agreed by the exporter and importer
  - A set of mandatory clauses which must always be included

International Data Transfer Agreement (IDTA)

- The ICO has published a draft addendum to the EC SCCs which can be used as an alternative to the IDTA
- Applies the EC SCCs in the context of UK data transfer - replacing references to the 'EU GDPR' with 'UK GDPR' etc
- This may be useful to organisations sending data from both the EU and the UK, enabling one set of SCCs to cover both transfers
- Consultation sought views on whether there would be value in publishing an IDTA for other jurisdictions e.g. New Zealand and ASEAN (Association of South East Asian Nations)
- Proposals seek a more pragmatic approach to data transfers than the more prescriptive model adopted by the EDPB

Transfer Risk Assessments

- The ICO has published a draft International Data Transfer Risk Assessment Tool (TRA)
- TRA structure not mandatory, but it has been structured to work alongside the IDTA and in three step process to assess…
  - The facts of the transfer
  - If the IDTA likely to be enforceable in the destination country
  - If there are appropriate protections in place for the data from third-party access
- Accompanied by guidance, decision trees and includes case studies and examples to help make appropriate assessment
- Assessment should determine whether the laws are 'sufficiently similar' to that in the UK to support the transfer

What does this mean for your data transfers?

- Until the IDTA is finalised, data transfers from the UK to non-adequate countries can be covered by the current UK SCCs
- The consultation proposes that they cease to be used:
  - 3 months after the IDTA enters into force for new transfers, and
  - 21 months after the IDTA enters into force for all existing UK SCCs

ACTION POINT

Review UK data flows and discuss a strategy and approach for international data transfers, look for announcements on the proposed documents that the ICO has published.

Session 2: ICO publications and announcements

Data sharing code of practice

- Published on the 17 December 2020
- Provides practical advice on how to carry out responsible data sharing
- ICO Elizabeth Denham said the COVID-19 pandemic brought the need for fair, transparent and secure data sharing into even sharper focus
- Provision for the code was included in the Data Protection Act 2018

> *"This code demonstrates that the legal framework is an enabler to responsible data sharing and busts some of the myths that currently exist.*
> *I want my code of practice to be part of a wider effort to address the technical, organisational and cultural challenges for data sharing. The ICO will be at the forefront of a collective effort, engaging with key stakeholders. I know I can count on a collective effort from practitioners and government to understand the code and work with the ICO to embed it."*
>
> Elizabeth Denham, ICO

Data sharing code of practice

- Organisations must follow the key data protection principles when sharing personal data:
  - Accountability i.e. being able to demonstrate compliance
  - Fairness and transparency
  - Identifying a lawful basis for sharing the personal data prior to sharing
  - Processing personal data securely with appropriate measures in place
- The code reveals how seriously the ICO considers its responsibilities in enforcing key risk areas
- Note the ICO's insistence on robust and well-documented risk assessments and recommendation to conduct DPIAs, even when not mandatory

Data Sharing Hub

Targeted support and resources, including:

- Data sharing myths busted
- Data sharing code basics for small organisations and businesses
- Data sharing FAQs for small organisations and businesses
- Case studies and checklists
- Data sharing request and decision forms template
- Sharing personal data with a law enforcement authority toolkit
- Guidance on sharing personal data with law enforcement authorities
- Guidance on data sharing and reuse of data by competent authorities for non-law enforcement purposes

ico.org.uk/for-organisations/data-sharing-information-hub/

Subject Access Requests

Updated Subject Access Request (SAR) guidance

- Revised guidance covers all aspects of the process of responding to subject access requests (SARs)
- The position on extending time due to complexity, carrying out searches of archived data and dealing with third party information are largely unchanged
- Particular focus on recognising SARs, exemptions and special rules for certain categories of personal data
- Provides clarity on the three key points:
  - Stopping the clock for clarification
  - What is a manifestly excessive request
  - What can be included when charging a fee for excessive, unfounded or repeat requests

Clock stops while clarifying the DSAR

- New guidance offers a "stop the clock" mechanism where clarification of the DSAR is **genuinely needed** in order for the data controller to carry out a reasonable search
- Should the data subject reply the same day, a data controller will not benefit from any extension of time
- Use of the mechanism is subject to a number of conditions…
  - Request for clarification should be made "as quickly as possible"
  - Clarification should only be sought where it is genuinely required in order to respond to the DSAR and where the controller processes a large amount of information
  - You must highlight the fact the clock stops and will resume on the day the individual responds

Manifestly excessive or unfounded requests

- A data controller can refuse to respond to all or part of a request if it is **manifestly unfounded** or **manifestly excessive**
- Data controllers cannot have a blanket policy and must assess each DSAR on its facts
- In determining whether a reasonable interval has elapsed, data controllers need to consider how often the data is altered
- A SAR may be **manifestly unfounded** if the individual has no intention to exercise their right or the request is malicious
- Needs strong justification and must be able to explain this to the data subject and ICO if needs be
- Each SAR must be assessed on its own merits

Manifestly excessive requests

- Consider whether it is clearly or obviously unreasonable by taking all the circumstances into account including:
  - The nature of the personal data, is it particularly sensitive?
  - The context of the request and relationship between the data controller and the data subject
  - The resources available to the organisation weighing up the burden, including costs, involved
  - Whether the SAR largely repeats previous requests and a reasonable interval has not elapsed
  - Whether it overlaps with other requests
- Requesting a large amount of information in itself will not make a SAR manifestly excessive

Charging for excessive, unfounded or repeated SARS

- A reasonable fee can be charged for the administrative costs of complying with a SAR if manifestly unfounded or excessive or an individual requests further copies of their data following a request
- A reasonable fee may include the costs of:
  - Transferring the information e.g. photocopying, printing, postage or providing access to an online platform
  - Equipment and supplies e.g. USB devices
  - Staff time at a reasonable hourly rate (no suggested rate)
- The costs must be explained clearly to the data subject
- No requirement to publish the criteria for charging fees online but should be clear, concise, accessible, and consistent

Practical implications

- If clarification is needed, data controllers must act quickly,
- They should also start the search exercise alongside, with a view to refining if and when the clarification is provided
- To ensure response deadlines can be calculated correctly keep logs of…
  - When SAR is received
  - When clarification is requested and provided
- The revised guidance on manifestly excessive SARs and the charging fees is helpful, but it will be a rare case that a data controller can justify relying on these provisions
- The ICO is planning a suite of further resources

Age appropriate design

Age appropriate design code of practice

- Came into Law on 1st September 2021 and comprises a set of 15 standards that online services should meet to protect children's privacy
- Applies to **online or connected products or services** that process personal data and are likely to be accessed by children in the UK (under 18)
- Requires automatic built-in baseline of data protection whenever they download a new app, game or visit a website
- Children should be treated differently depending on their age group e.g. 0-5, 6-9, 10-12, 13-15 or 16-17

- Apps
- Connected toys
- Social media platform
- Online games
- Educational websites
- Streaming services

What does this mean in practice?

- Privacy settings should be set to high by default
- Nudge techniques should not be used to encourage children to weaken their settings
- Location settings that allow the world to see where a child is, should also be switched off by default
- Data collection and sharing should be minimised
- Profiling that can allow children to be served up targeted content should be switched off by default

Compliance steps

- Double check your audience and the steps you take to screen out and/or protect children
- Ensure all optional data collection/sharing settings are off by default for all users under 18 in the UK
- Ensure you provide child friendly privacy disclosures in your privacy policy and "just-in-time" notices
- Document compliance through a Data Protection Impact Assessment (DPIA) (as required by the Code)
- Consider how child privacy fits into a larger compliance program
- Check with your certification provider about compliance with the Code

Employer guidance

Employer guidance from the ICO

- The ICO has previously published detailed guidance, including the employment practices code, supplementary guidance and the quick guide
- They plan to create a hub of guidance covering various employment topics and issues including…
  - Processing of personal data in the context of recruitment
  - Selection and verification
  - Employment records
  - Monitoring at work and workers' health
  - Data processing in the context of TUPE
- This will be done in various ways including consultations on significant pieces of guidance as they are developed

Other raised areas of concern…

- Lawful basis and conditions for processing
- The impact of the COVID-19 pandemic
- Data sharing
- Equal opportunities monitoring and diversity and inclusion
- Applications and interviews
- Social media and other publicly available sources
- Monitoring of workers (remotely and in the office)

Accountability toolkit

ICO accountability toolkit

"Organisations must understand the risks they create for individuals when processing their data and mitigate against those risks. Organisations must be able to demonstrate that they handle personal data appropriately and effectively. These actions are all a part of the data protection requirement of accountability.

The principle of accountability is really about putting data protection at the heart of all personal data processing. It means being crystal clear about data protection responsibilities across the entire organisation; data protection being a boardroom issue and not just the responsibility of the data protection officer; managing risk proactively; and being transparent with people about what you are doing with their data."

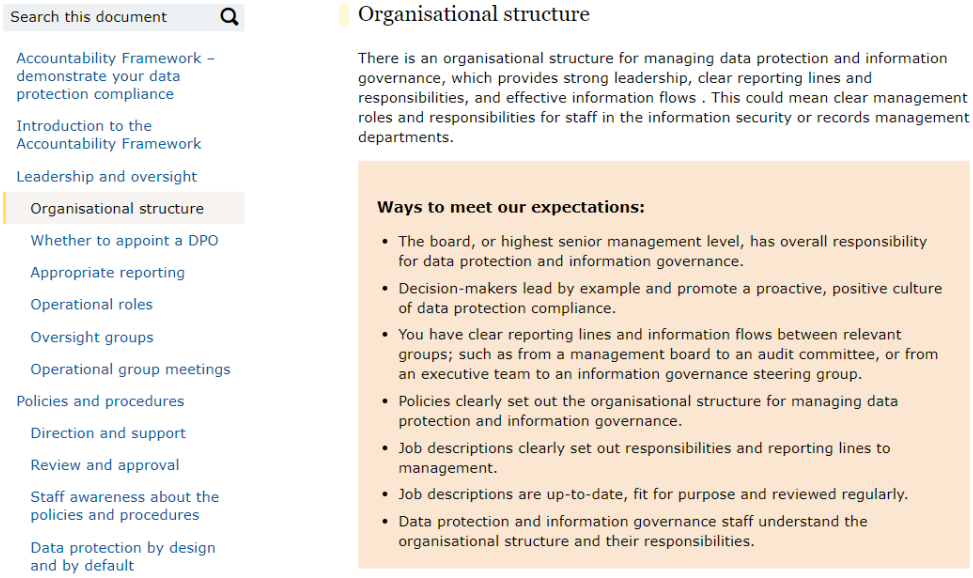
Ian Hulme, Director for Regulatory Assurance

What is the accountability toolkit?

- Toolkit launched in September 2020
- Supports organisations in demonstrating their compliance with the accountability principle to the ICO, the public or their business partners
- Illustrates how central accountability is to all collecting and processing personal data
- Ten categories (77 sub-categories) in the framework…
  - Each sets out the expectations the ICO has about how the category should be complied
  - Additional detail about ways in which those expectations can be met is also provided

Accountability toolkit categories

1. Leadership and oversight
2. Policies and procedures
3. Training and awareness
4. Individuals' rights
5. Transparency
6. Records of processing and lawful basis
7. Contracts and data sharing
8. Risks and data protection impact assessments
9. Records management and security
10. Breach response and monitoring



ico.org.uk/for-organisations/accountability-framework

ACTION POINT

Review current procedures against the guidance issued by the ICO and regularly check for new and updated guidance.

Session 3: UK and EU Enforcement Activity

No Win No Fee?

Examples of the types of workplace data breaches we can assist with include:

- Documentation left in communal work areas or on communal printers
- Information being sent to incorrect email recipients – both internally and externally
- Employers or employees misusing confidential data relating to other employees, customers and any other individuals
- Personal data being accessed in a cyber attack caused by employer or employee negligence
- Failure to properly dispose of confidential data leading to this data falling into the wrong hands

Type of breach	Estimated potential compensation
Breach of an individual's name, date of birth, home and email addresses	£1,000 - £1,500
Breach of medical records	£2,000 - £5,000
Breach of financial information	£3,000 - £7,000
Breach which causes depression or illness (Medical evidence would be required to support this along with evidence to support any other losses, for example earnings)	£25,700 - £42,900

Warren v DGS Retail

- DGS Retail suffered a cyber attack and the ICO took enforcement action against them
- The causes of action relied upon by the claimants were:
  - Breach of the Data Protection Act 1998
  - Misuse of private information
  - Breach of confidence
  - Negligence
- Court held that a misuse of private information still required a "use": that is, a positive action
- It was concluded that it was not the defendant that disclosed the claimant's personal data, or misused it, but the
  criminal third-party hackers

- The claim in negligence was considered to be problematic, for two reasons:
  - There is no need nor warrant to impose such a duty of care where the statutory duties under data protection law operate
  - A claim in negligence could only succeed where damage had been suffered and a state of anxiety falling short of a clinically recognisable psychiatric illness does not constitute damage for these purposes
- On that basis, the judge determined that the claim in negligence was to be dismissed and/or struck out

Johnson v Eastlight

- The case concerned data breach involving an email error
- The claimant brought a case in the High Court for Misuse of Private Information, Breach of Confidence and negligence (the latter was later withdrawn) together with a Human Rights Act and DPA 2018 claim for damages of £3,000 and costs of £50,000
- The judge rules that there was no basis for the claim to have been issued in the High Court and stated *"The presentation and processing of this case to-date in this forum has, I am satisfied, constituted a form of procedural abuse."*
- Reluctantly, the judge agreed to transfer the case to the County Court rather than strike it out in its entirety

Rolfe v Veale Wasbrough Vizards

- A letter requesting the payment of school fees was sent to a person with an identical surname and the same first initial
- The Claimants brought a claim for damages in the High Court
- The judge dismissed the claim and strongly cautioned against bringing such claims in the High Court:
- *"In my judgment no person of ordinary fortitude would reasonably suffer the distress claimed arising in these circumstances in the 21st Century, in a case where a single breach was quickly remedied…the law will not supply a remedy in cases where effectively no harm has credibly been shown or be likely to be shown."*

Ashley v Amplifon Ltd

- A data breach case concerning the inadvertent disclosure to the wrong employee (with the same first name) of an employment contract
- The judge held that there were factual matters to be resolved in the County Court, not the High Court
  "I would not deny the claimant access to the county court, probably the small claims track, to litigate the claim. Access to justice includes the right to litigate modest claims for amounts that may seem trivial to lawyers but are not to the party seeking not just the money but to vindicate their rights. Whether the claim is worth the candle must be seen in that light."

Lloyd v Google

- On 10th November 2021, the UK Supreme Court in a unanimous judgment allowed Google's appeal against the previous Court of Appeal decision
- Reversing the decision of the Court of Appeal, the Supreme Court unanimously held that damages are not awardable for a mere loss of control of personal data under the old DPA regime: it held that
  "[Section 13 of the DPA] cannot reasonably be interpreted as giving an individual a right to compensation without proof of material damage or distress whenever a data controller commits a non-trivial breach of any requirement of the [DPA]..."

What does all of this mean?

- The High Court criticism of distress based claims and the Supreme Court's ruling in Lloyd, send a very clear message
- Not every data breach or unlawful processing of personal data is capable of giving rise to compensation
- The Lloyd judgment is not the end of representative actions, but the time and cost involved may well deter claimant firms
- The firm tone taken by judges in recent cases is indicative of the High Court's approach to trivial data breach claims
- Multiple causes of action continue to be referenced by claimant firms but the clear message is the judiciary will not wave through such claims and award damages where no real distress has been caused

ICO and Clearview

- On 29th November 2021, the ICO announced provisional intent to impose a potential fine of just over £17 million on Clearview AI
- Also issued a provisional notice to stop further processing of the personal data of people in the UK and to delete it
- The investigation focused on Clearview's use of images, data scraped from the internet and the use of biometrics for facial recognition
- Many companies considering facial recognition technology through desire to have "touch free" access in smart devices
- Enforcement highlights the importance of ensuring companies have appropriate notice and consent from data subjects and maintain adequate privacy compliance programs

ICO and Clearview

Preliminary view is that Clearview appears to have failed to comply with UK data protection laws in several ways including…

- Failing to process the information of people in the UK in a way they are likely to expect or that is fair
- Failing to have a process in place to stop the data being retained indefinitely
- Failing to have a lawful reason for collecting the information
- Failing to meet the higher data protection standards required for biometric data
- Failing to inform people in the UK about what is happening to their data

"I have significant concerns that personal data was processed in a way that nobody in the UK will have expected. UK data protection legislation does not stop the effective use of technology to fight crime, but to enjoy public trust and confidence in their products technology providers must ensure people's legal protections are respected and complied with.
Clearview AI Inc's services are no longer being offered in the UK. However, the evidence we've gathered and analysed suggests Clearview AI Inc were and may be continuing to process significant volumes of UK people's information without their knowledge. We therefore want to assure the UK public that we are considering these alleged breaches and taking them very seriously."

Elizabeth Denham

GDPR fines

- Since May 2018 there have been 940 fines issued totalling €1,556,179,408*
- Largest fines to date:
  - Amazon - €746 million ($877 million)
  - WhatsApp - €225 million ($255 million)
  - Google – €50 million ($56.6 million)
  - H&M - €35 million ($41 million)
  - TIM – €27.8 million ($31.5 million)
  - British Airways – €22 million ($26 million)
  - Marriott – €20.4 million ($23.8 million)

**as of January 2022*

WhatsApp

- Ireland's Data Protection Commission (DPC) has fined WhatsApp €225 million for failings of transparency under EU data protection laws
- Ordered the company to amend its practices within three months
- Final fine imposed of €225m is much greater, reflecting interventions made by other European authorities
- Additional findings of infringement made by the EDPB including breaching the transparency principle
  - On its own accounts for €90m of the overall final fine imposed
- Fine factored in the turnover of all the companies falling under the umbrella of Facebook In - WhatsApp's parent company
- The DPC had argued that Article 83(3) restricted it to capping its total fine no higher than "the amount specified for the gravest infringement" – this being the breach of Article 14
- However, the EDPB disagreed…
  "when faced with multiple infringements for the same or linked processing operations, all the infringements should be taken into consideration when calculating the amount of the fine, provided that the level of fine is proportionate and does not exceed the maximum penalty that can be imposed under the GDPR."

Facebook

- In October 2021 the Irish DPC proposed up to $42 million in fines for Facebook for failure to provide clear information about their legal basis for processing
- Facebook have unique approach by including data processing specifications in general T&Cs and interprets the agreement as a contract rather than consent
- Draft decision endorsing Facebook's legal basis for processing personal data will be sent to authorities
- Certain that they will challenge, triggering the dispute resolution mechanism
- Negative decision on the contractual approach would have disastrous consequences for its business model
- Facebook's primary source of income is targeted advertising - harvesting and processing vast amounts of data
- Facebook Ireland set aside €302 million for possible fines
- December accounts filing states states the provision represents the "best estimate" of what the potential liability could be
- Facebook believes compliance costs and fines could range between €154 million and €541 million
- Expects the matters to be resolved within the next 2 financial years
- Facebook currently being investigated in 11 statutory inquiries by the Irish data regulator: 8 Facebook, 2 WhatsApp and 1 Instagram

Swedish retailer H&M

Hamburg DPA issued €35.3 million fine for the GDPR violation…

- Collected sensitive personal data of their employees to create detailed profiles including medical records – diagnoses & symptoms and private details about vacation and family affairs
- Used to help evaluate employees' performance and make decisions about their employment
- Senior staff gained *"a broad knowledge of employees' private lives… from harmless details to family issues and religious beliefs."*
- A technical error resulted in the data being accessible to everyone in the company for a few hours
- The press picked up the news made the Commissioner aware

ACTION POINT

Ensure senior managers are aware of the courts approach in recent compensation claims.

Session 4: Marketing

ICO – Draft marketing code of practice

- Public consultation ran from 8th January to 4th March 2020
- The ICO intends the new code to apply to all processing of data for *"direct marketing purposes"* and aims to…
  - Provide practical guidance
  - Promote best practice for processing data for direct marketing purposes in compliance with data protection/e-privacy rules
- Once adopted, the ICO will monitor compliance through proactive audits

***Remember** – you will likely need to follow the new guidance if you're collecting or using data for direct marketing*

What are the key proposals?

- **Direct marketing messages** - reiterates that GDPR will apply irrespective of the method used
- **Social media platforms** - provides guidance when using to target direct marketing at individuals
- **Tracking** - use of location-based marketing techniques must be transparent
  - It will be difficult to demonstrate the legitimate interests requirement
- **Service messages** – where sent to an individual, consent is not required E.g. alert of mobile data usage

What are the key proposals?

- **Viral marketing "tell a friend campaigns"** - likely to breach the PECR as the instigating organisation…
  - Has no direct contact with the ultimate recipients
  - Will not know what the referring individual has told their friends about the processing *and*
  - Will not be able to verify whether the friend provided GDPR standard consent
- **Publicly available information**
  - If collected by an organisation, it must still comply with the GDPR and PECR as a controller
  - Individual posting details on social media is not an agreement to content being analysed/profiling for direct marketing purposes

Adtech - background

- ICO engaged with the advertising industry throughout 2019 and an interim report was produced in June 2019
- Justifications for the use of legitimate interests as the lawful basis for the processing in Real Time Bidding (RTB) were considered insufficient by the ICO
- DPIAs deemed to be…
  - Generally immature
  - Lacking detail
  - Not following the ICO's recommended steps to assess the risk to the rights and freedoms of the individual
- UK advertising trade bodies have agreed to produce guidance for their members

Data protection and privacy expectations for Adtech from the ICO

November 2021 Opinion outlines **principles** which any adtech solution, proposal or initiative should meet:

- **Data protection by design** should be incorporated during the design phase
- **User choice** should allow meaningful control and the ability to exercise data subject rights
- **Accountability** should exist across the lifecycle of the processing supply chain
- **Purposes** of data processing should be clearly articulated, necessary and proportionate
- **Reducing harm** by ensuring that privacy risks are addressed (DPIAs)

- Proposals looking to replace cookies and similar technologies need to "raise the standards of data protection and privacy, and not dilute them"
- Opinion sets out key recommendations that developers can take to address risks prior to deployment:
  - Demonstrate and explain design choices
  - Be fair and transparent about the benefits
  - Minimise data collection and further processing
  - Protect users and give them meaningful control
  - Demonstrate necessity and proportionality
  - Consider lawfulness, risk assessments and information rights
  - Mitigate risks of processing special category data

Cookies and online tracking technologies – CNIL draft code of practice

Launched in October 2020 – CNIL recommends to…

- List each purpose with a short and prominent title (bold/underlined), accompanied by a brief description of the purpose
- Provide this information in the cookie banner or panel
- Provide more detailed information about the purposes through a scroll-down feature or separate screen that is easily accessible from the consent collection interface (e.g. a link)
- In the case of multiple controllers, provide an exhaustive and up-to-date list of controllers
  - Permanently and easily accessible
- Request new consent in case of substantial changes to this list
- Inform users whether their consent will allow the tracking of users' browsing behavior across different websites and applications
  - If the case, the names of those websites and applications

CNIL also provide specific guidance on obtaining the user's consent…

- Must be freely given
- Specific to the purpose
- Indicated through an affirmative and clear action by the individual
- Easy to withdraw at any time
- Documented

- Users should only be offered the possibility to consent to all cookies at once if they are also offered the possibility to consent to specific cookies per purpose and to refuse all cookies at once
- A website or application should keep evidence of the user's consent obtained and of the consent interface used

Fines for Facebook and Google

31 December 2021 - French Data Protection Authority (CNIL) imposes fines on Google and Facebook…

- Background
  - Businesses given 6-month transition period to comply with cookie guidelines until 31 March 31 2021
  - After complaints, CNIL investigated the cookie practices of Facebook, Google and Youtube
- CNIL conclusions
  - The websites offered an easy way to consent to the cookies immediately after accessing the websites, but not an equally easy way to refuse the use of cookies
  - Facebook provided unclear and confusing instructions on how to refuse cookies
- Sanctions
  - Imposed €150m fine on Google and €60m on Facebook
  - Ordered Facebook and Google to provide French users with a method to refuse cookies that is as easy as the method to consent to cookies within 3 months of the decision
  - Failure to do so will result in daily penalties of €100,000

Recent EU cases

- December 2021 – Google fined €150m
- December 2021 – Facebook fined €60m
- December 2020 - Google fined €135m
- December 2020 - Amazon fined €35m
- November 2020 – Carrefour fined €3.7m
- October 2019 – Spanish DPA fined Vueling €30,000
- December 2019 - the Belgian DPA fined Jubel €15,000

ACTION POINT

Review use of cookies and other advertising technology and ensure use is compliant with revised guidance and developing case law.

Session 5: Conclusion

Summary of recommended actions

- Review UK data flows and discuss a strategy and approach for international data transfers, look for announcements on the proposed documents that the ICO has published.
- Review current procedures against the guidance issued by the ICO and regularly check for new and updated guidance.
- Ensure senior managers are aware of the courts approach in recent compensation claims.
- Review use of cookies and other advertising technology and ensure use is compliant with revised guidance and developing case law.

Appendix 1 – Further guidance

ICO Guide to the GDPR	www.uktraining.com/18pla
ICO GDPR Checklists	www.uktraining.com/18plb
FAQs for small organisations	www.uktraining.com/18plc
FAQs for charities	www.uktraining.com/18plf
FAQs for the education sector	www.uktraining.com/18pld
FAQs for the health sector	www.uktraining.com/18ple
European Commission DP page	www.uktraining.com/18plg
EDPB Guidance	www.uktraining.com/18plh

Appendix 2 - Privacy principles in practice

In practice you should always follow these guidelines when processing personal data…

- Personal data may only be processed in a lawful and correct manner and in accordance with your Privacy Policy
- Personal data may only be processed for specific and clearly stated purposes
  - Personal data may not be collected or used arbitrarily
- All personal data collected must be relevant for the specific purpose
  - No more data may be collected than is necessary for the specific purpose
- Personal data must be correct and updated
  - If it is discovered that personal information is incorrect or processed in a way that violates policy, the information will be corrected or deleted
- Before a data subject's personal data is processed, it must be determined when and how to inform them about the processing of their personal data
  - Personal data may only be processed if such information has been provided
- Personal data may not be retained longer than necessary for the intended purpose
- Personal data should be protected appropriately
  - The organisation always ensures that there is an appropriate level of security for personal data
  - Personal data should only be available and used by relevant personnel within the organisation who need the information to perform their duties

Appendix 3 - ICO examples of 'High Risk' processing

1. **Innovative technology**
   - Processing involving the use of innovative technologies, or the novel application of existing technologies (including AI)
2. **Denial of service**
   - Decisions about an individual's access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data
3. **Large-scale profiling**
   - Any profiling of individuals on a large scale
4. **Biometrics**
   - Any processing of biometric data. A DPIA is required where this processing is combined with any of the criteria from the European guidelines
5. **Genetic data**
   - Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject
   - A DPIA is required where this processing is combined with any of the criteria from the European guidelines
6. **Data matching**
   - Combining, comparing or matching personal data obtained from multiple sources
7. **Invisible processing**
   - Processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort
8. **Tracking**
   - Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment
9. **Targeting of children or other vulnerable individuals**
   - The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children
10. **Risk of physical harm**
    - Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals

UK Training (Worldwide) Limited
17 Duke Street
Formby
L37 4AN

w www.uktraining.com
t 01704 878988
e info@uktraining.com