UKTraining

GDPR: The Essential Update

Course book

…market leaders for business training

Course book

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

GDPR: The Essential Update

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

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

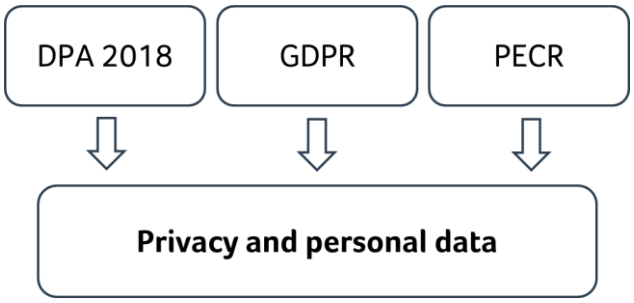
Contents

Session 1: The data protection landscape

What are the objectives of privacy and data protection laws?

- Protect the fundamental rights and freedoms of living individuals with regard to privacy and personal data
- Enable the free movement of data between states that have an adequate level of protection
- Set out the rules by which personal data can be accessed or used by agencies of the Government
- Balance the needs of organisations against the rights of individuals

The'old' data protection regime



Brexit

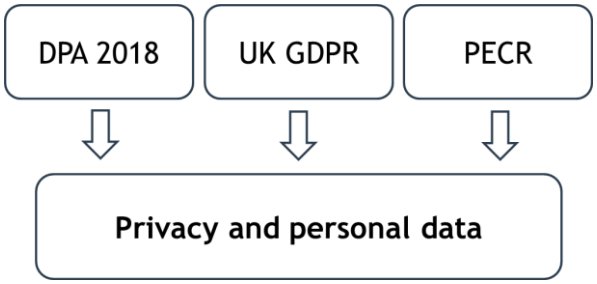
- The UK has left the EU and is no longer regulated domestically by the EU GDPR
- The UK now has its own version - the UK GDPR (United Kingdom General Data Protection Regulation)
  - Created by the European Union (Withdrawal) Act 2018
  - Updated by the Data Protection, Privacy and Electronic Communications (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

Brexit and the UK GDPR

- The UK GDPR is established by the European Union (Withdrawal) Act 2018 as it existed on 30 January 2020 – 'exit-day'
- The EU Exit Regulations applies a number of changes to the GDPR to make it relevant to the UK following departure from the EU…
  - Removes references to cross-border data transfers with other Member States and participation in EU wide-institutions such as the EDPB
  - Deals with the arrangements for the UK to adopt its own adequacy decisions and contractual safeguards for data transfers

The 'new' data protection regime

UK GDPR, DPA 2018 and PECR are applied jointly



UK GDPR – what is different?

- Core definitions and legal terminology are the same as the EU GDPR
- Personal data, rights of data subjects, legal bases for processing, controller, processor, etc. are in the UK GDPR
- Personal data of data subjects outside the UK that was acquired before 31 December 2020 ('legacy data') will continue to be subject to the EU GDPR as it stood on that date ('frozen GDPR')
- The frozen GDPR will be as interpreted by the European Court whereas UK GDPR is interpreted by the UK courts

What is different?

- UK GDPR does expand on the EU GDPR in some areas:
  - **National security**
  - **Intelligence services**
  - **Immigration**
- The ICO is now the leading supervisor, regulator and enforcer of the UK GDPR
- The Secretary of State now has powers to determine or revoke adequacy decisions on behalf of the UK GDPR
  - Can make these decisions without the consultation of the ICO
- **Valid consent** is lowered to 13 in the UK (16 in the EU)

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 (by EU Data Protection Authorities in the EU and the ICO in the UK) in the event of any breach
- 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
- The UK/EU Trade Agreement varies this position through a bridging mechanism
- EU to UK transfers of personal data will not be considered a transfer to a third country for up to six month (June 2021)
- While nothing further is required immediately, keep this under review
  - The ICO recommends putting in place alternative transfer mechanisms to safeguard against any interruption to the free flow of EU to UK personal data

- The UK GDPR automatically recognises all EU countries as adequate, along with recognising 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

Practical steps

- **Map data flows:** Ensure details of data flows between the EU and UK have been mapped out to help assess and take appropriate next steps to comply with the two GDPR regimes
- **Update records of processing:** Update records to meet EU and UK GDPR requirements
- **Re-evaluate lead supervisory authority:** Assess impact of dealing with a new EU supervisory authority or multiple authorities i.e, notifying a security breach
- **Appoint a UK and/or EU representative:** Are you offering goods or services, or monitoring the behaviour of individuals in the EU or vice versa

- **Update privacy notices:** Revise internal and external privacy notices to ensure they cover the relevant requirements of the UK GDPR and differentiate where necessary
- **Amend existing contracts and templates:** Update terms to include relevant data transfer wording and appropriate referencing to the UK and EU GDPR
- **Consider whether DPIAs need to be updated:** Existing data protection impact assessments may need to be updated to ensure they comply with the UK GDPR

The future…

- The UK government is currently consulting on its National Data Strategy
- UK data protection law is likely to be amended in the coming year
- International transfers of personal data appear high on the agenda (following the end of the bridging period)
- The ICO has also indicated that there will be a consultation on new UK standard contractual clauses for data transfers

International transfers

- Data exporters can use existing EU versions of standard contractual clauses, either 'as is', or with the limited changes needed to reflect the UK's withdrawal from the EU
- The expectation is that the ICO will approve a new set of standard contractual clauses
  - Likely to replicate and align with the new draft standard contractual clauses published by the European Commission in November 2020
- Transfer arrangements will need to take account of the CJEU decision in Schrems II and guidance provided by the EDPB and ICO

Privacy shield

- Ruled unlawful by the CJEU in July 2020
- No grace period was granted
- Transfers of personal data to the US are now the same as any other country that does not have an 'adequacy' decision
- The EDPB recommend you conduct a risk assessment to decide whether SCCs provide enough protection within the local legal framework
- The ICO have promised further guidance

EDPB guidance

Six steps recommended on the approach to any transfer of data…

1. **Know your transfers** - exporting controllers and processors ought to know what data they are sending, to whom, and where it resides
2. **Verify the transfer tool** - SCCs, or potentially binding corporate rules (**BCRs)** or an adequacy decision
3. Assess the legal safeguards in the destination country
4. Identify and adopt supplementary measures
5. **Take formal procedural steps** - address any necessary procedural steps following steps 3 and 4
6. Keep it all under review - The position may change

Undertaking a transfer assessment

- The exporter must consider the specific characteristics of each transfer to determine the laws applicable
  - The exporter will need to determine:
  - Whether the applicable laws specific to its transfer are likely to require the disclosure of transferred data to, or permit access of data by, public authorities
  - Whether these requirements or powers are limited to what is "*necessary and proportionate in a democratic society*" (measured against the EDPB European Essential Guarantees)
- Many organisations will probably look to what effective supplementary measures may be required to protect the transfer

Supplementary measures

- Annex 2 of the recommendations provides a non-exhaustive list of supplementary measures:
  - Technical – encryption, pseudonymisation
  - Contractual – clauses requiring transparency, reviews and notifications by the importer
  - Organisational – internal policies, accountability measures
- Practical steps
  - Develop an approach on conducting transfer risk assessments
  - Consider what additional measures make sense
  - Be prepared to negotiate with your vendors to ask for some of the contractual promises set out
  - Document why you think those measures suffice

Supplementary measures

- Annex 2 of the recommendations provides a non-exhaustive list of supplementary measures:
  - Technical – encryption, pseudonymisation
  - Contractual – clauses requiring transparency, reviews and notifications by the importer
  - Organisational – internal policies, accountability measures
- Practical steps
  - Develop an approach on conducting transfer risk assessments
  - Consider what additional measures make sense
  - Be prepared to negotiate with your vendors to ask for some of the contractual promises set out
  - Document why you think those measures suffice

ACTION POINT

Identify transfers from the UK and determine appropriate form of safeguarding.

Session 2: Accountability

ICO view…

"Accountability encapsulates everything the GDPR is about. It enshrines in law an onus on companies to understand the risks that they create for others with their data process In practice, this means that organisations need to ensure that they not only have appropriate policies and procedures in place but that they can demonstrate through risk assessment, audit and review that that the processes being adopted meet the standards of the GDPR and the UK's new Data Protection Act of 2018 and to mitigate those risks. **It is a legal requirement, it is not optional.**"

"**Essentially, the culture of compliance should be within the DNA of the business**. There is inherent danger in businesses taking a formulaic or generic approach to their GDPR obligations."

"This next phase of GDPR requires a refocus on comprehensive data protection – **embedding sound data governance in all of your business processes**."

Elizabeth Denham, 25 May 2019

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

- 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 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

ICO 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

Accountability

Principles Controller must be able to demonstrate compliance with the six privacy principles
Data Processing Records Requirement to maintain records of data processing activities
Security Implement appropriate technical and organisational measures to protect personal data
Privacy by Design Consider data protection from the start of the project and integrate safeguards into design of the service
Privacy by Default Collect, process and store the minimal amount of data necessary and ensure that it is only accessible by authorised individuals
Data Protection Officer Formal requirement to appoint a DPO if organisation falls within stated criteria
Data Protection Policies Documented policies are required to demonstrate adherence to requirements of GDPR
Joint Controllers Must transparently agree their respective responsibilities for compliance with GDPR requirements (subject rights, processing notices)
Processor Contract Processors must operate under a written contract containing the terms laid out in Article 28
Adherence to Standards Adherence to approved codes of conduct or certifications may be used to demonstrate compliance with these obligations

The core principles in Article 5 of GDPR

Data should be…

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and, where necessary, kept up to date
5. Retained only for as long as necessary
6. Processed in an appropriate manner to maintain security

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
  - That personal data should only be available and used by relevant personnel within the organisation who need the information to perform their duties

Penalties and enforcement under DPA 2018

- For (mainly) a breach of record keeping, contracting and security clauses
  - Maximum fine of up to €10 (£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 €20 (£17) million, or 4% of annual worldwide turnover, whichever is greater
- EU DPAs intend to co-ordinate their supervisory and enforcement powers across the Member States

CNIL and Google

- Commission nationale de l'informatique et des libertés (CNIL) found information provided by Google was not complete and did not comply with principles of accessibility, clarity or intelligibility
- CNIL noted
  - Information “scattered” across several documents
  - Difficult to “easily access entirety of information”
  - 5 actions required to get information about Ads personalisation processing
  - Retrieving information was difficult “even for privacy professionals”

CNIL and Google

- Google was heavily sanctioned for failing to specify the period of time it would retain the personal data

> *"It is mandatory for this information to be provided to the persons concerned pursuant to Article 13 (2) of the Regulation"*

- CNIL found Google did not have a legal basis for processing under Article 6
  - Valid consent - informed, specific or unambiguous – had not been obtained

Fine = €50 million

The lawfulness, fairness and transparency principle

- There must be a legal basis for processing
- Processing must be in compliance with all laws
- Transparency is key to 'fairness'
- Typically this means notice to the individual as set out in Articles 13 and 14

Privacy notices to Data Subjects – *Summary of Articles 13 and 14*

- Identity and contact details of Data Controller
- What data is being processed?
- Purposes of the processing of the data
- Legal basis for processing
- If 'legitimate interests' used, what those 'legitimate interests' are
- Recipients or categories of recipients - any Processors
- The categories of personal data obtained if the personal data is not obtained from the Data Subject directly

- International data transfers and on what basis (adequacy finding, suitable safeguards etc.)
- Retention period or criteria applied
- Individual rights under GDPR
- Whether a statutory or contractual requirement
- Existence of automated decision making and logic involved
- How to make a complaint
- Details of the DPO if one is required

UODO and Bisnode (Swedish based-data broker)

- Gathered information about sole traders and company directors/officers from public registries
- Provided privacy notice to approximately 650,000 sole traders whose email address was available in the public database
- Decided not to provide the notice to sole traders without an email address
- Cost of sending registered letters too high – PLN 33.5m or almost €8m – 97% of turnover - Instead published the notice on their website
- Relied on exemption under article 14(5) - providing the notice to all sole traders would cause disproportionate effort

UODO (Polish DPO) response…

- Did not accept this reasoning
- Company had postal addresses – could notify with a standard letter without confirmation – reduce cost
- Emphasised that the rights of sole traders prevail
- Bisnode should have taken into account the cost of notification in their business model

They were fined PLN 1m (230,500 euros) and given 90 days to notify the sole traders

Lessons from Bisnode

- Polish court upheld decision on the 11 December 2019 - first GDPR court decision
- Strict interpretation of Article 14
- Bisnode elected to delete the data of 7 million people - enforcement action would cost significantly more than the fine
- DPA stated that there is no particular means of fulfilling the obligation to inform - it just requires the data controller to actually reach out
- Reinforces the need to actively provide privacy information to data subjects rather than passively publish it on websites
- Also reminds that information relating to people in their business or professional capacity is still personal data

Privacy by design and default

Privacy by design

- Each new service or business process that makes use of personal data must take the protection of such data into consideration

Privacy by default

- The strictest privacy settings automatically apply once a customer acquires a new product or service

Data Protection Impact Assessments (DPIA)

- A DPIA is an assessment that is undertaken to identify potential areas of non-compliance and minimise the risk
- Under GDPR, a DPIA must be carried out before beginning any new 'high-risk' processing activity
- DPIAs should include the following as a minimum
  - A description of the processing activity and the purpose
  - An outline of the risks and the measures taken in response
  - The formal advice of the DPO (if appointed)

ICO example of 'High Risk' processing

1. Innovative Technology
2. Denial of Service
3. Large Scale Profiling
4. Biometric Data
5. Genetic Data
6. Data Matching
7. Invisible Processing
8. Tracking
9. Targeting children or vulnerable adults
10. Risk of physical harm

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

ICO example of 'High Risk' processing

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

Datainspektionen and Skelleftea municipality

- Swedish school in the Skelleftea municipality ran a pilot scheme to monitor attendance using CCTV and facial recognition software
- Tracked 22 students in and out of classrooms over 3 weeks
- Municipality claimed teachers spent 17,000 hours a year reporting attendance
- Scheme designed to see whether facial-recognition technology could speed up the process
- School obtained parents' consent to monitor the students

Swedish DPA response…

- Fined Skelleftea municipality 200,000 Swedish Krona (£16,800) for breaching article 35
- Not legally adequate reason to collect sensitive personal data
- Although some parts of school could be considered 'public', students had an expectation of privacy in the classroom
- Less intrusive ways of monitoring attendance

Skelleftea's local authority had **unlawfully processed sensitive biometric data** and **failed to complete an adequate DPIA**, which would have included consulting the regulator and gaining prior approval before starting the trial

Final word

"Accountability not only drives the GDPR but is also a critical component of data protection and privacy law, regulation, and industry guidance across the world."

"It captures in law an onus on companies to understand the risks, and to mitigate those risks. It also reflects that people are increasingly demanding to be shown how their data is used and how it is being protected."

"**Accountability requires a change of culture within organisations, and the bedding in of key governance systems and values**. We know from our investigations and audits that this has not happened yet. **We will therefore be doing more to ensure that this happens**. What is clear however is the wider ambition for progress in this area."

Steve Wood, 20 May 2019

ACTION POINT

Review current procedures against the accountability principle and ensure compliance can be demonstrated.

Session 3: Data Subject Rights

Data subject rights

- Access
- Rectification
- Erasure ('Right to be forgotten')
- Restriction of processing
- Portability
- Object to processing
- Automated decision making, including profiling
- Compensation

Access

- An individual who makes a written request is entitled to be told whether or not any of their personal data is being processed
- If this is the case they are entitled to the following information:
  - A description of the personal data, the purposes for which it is being processed, recipients, retention period and rights of rectification, erasure, restriction and objections
  - Existence of automated decision making
  - Transfer safeguards
  - A copy of the information comprising the data; and given details of the source of the data (where this is available)

Access

- No fee is payable for subject access requests
- Information must be supplied within **1 month**
  - Requests that are 'complex' or 'numerous' may be allowed a further 2 months to comply
- Can include opinions, voice recordings and manual records
- Very few exemptions
- You can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive
  - The fee can only cover the administrative costs

ICO code of practice

- Published October 2020
- The updated guidance particularly focuses on:
  - Recognising DSARs
  - Exemptions
  - Special rules for certain categories of personal data
  - How to deal with requests involving the personal data of others
- 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

Recent EU court cases

Two recent cases in Germany and The Netherlands confirmed:

- The right of access under the GDPR is not materially different to the Data Protection Directive
- The GDPR does not grant a right to obtain a copy of documents, it only grants a right to obtain a copy of personal data
- The information provided should be sufficient to allow the data subject to verify the correctness of the data and its lawful processing
- For documents that do not contain much personal information, such as emails, it suffices to describe the data they contain
- In GDPR terms, "copy" has the meaning of "a summary of the personal data structured in a meaningful way" not a "photocopy" or a "data set"

ACTION POINT

Review DSAR procedures in light of recent cases and ICO draft guidance.

Session 4: Breaches and penalties

What is a data breach?

- The GDPR contains a definition of a data breach, which was not present in the preceding legislation

> *A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed*

Data breach notification

When a data breach occurs…

- Notify appropriate Supervisory Authority
  - Where feasible within 72 hours
  - Unless breach is unlikely to result in risk to individuals
- Requirement to notify individuals without undue delay if breach is likely to result in high risk to the individuals affected

Data breach record keeping

- Under the principle of Accountability **all** breaches should be documented, even when notification is not required
- An internal breach register or log should include the following…
  - Date and time
  - The facts of the case
  - Effects and consequences
  - Remedial actions
  - Reasoning for actions taken
  - Reasoning for not notifying, where applicable

Recent breaches

- **1,687,470,669** non-sensitive records exposed (email addresses, usernames, passwords)
- **446,515,334** number of consumer records exposed containing sensitive personally identifiable information in the US
- **426,367,432** records exposed as a result of unauthorised access and accidental exposure

Identity theft

- In the UK, 500 identity fraud cases are reported every day
- $96m credit card fraud in the US last year
- Fullz – hacker slang for "full ID" package
  - Name, address, online passwords, banking data and other key identifying information
  - Typically worth £820 each on the dark web
- Criminal Guides for sale on dark web marketplaces, e.g.
  - £6 "How to obtain loans guide", which gives step-by-step instructions on how to take out a loan using stolen data

- According to the UK police fraud division, identity theft is used to:
  - Open bank accounts
  - Get credit cards, loans, and state benefits
  - Take over existing accounts
  - Order goods in your name
  - Get passports, driving licenses and personal documents
  - Take out mobile phone contracts

The Information Commissioner's Office (ICO)

- The ICO was established in 2001 and is the statutory regulator for information, privacy and data protection in the UK
- Responsibilities include…
  - Maintaining a register of Data Controllers and Processors
  - Upholding information rights and enforcing legislation such as GDPR, DPA 2018, PECR, FOIA and others
  - Handling concerns and dealing with complaints
  - Providing guidance
  - Collaborating internationally
  - Reporting to Parliament

ICO and British Airways

- On 16 October 2020 the ICO fined British Airways £20 million for infringements of GDPR
- Cyber incident involving user traffic to the BA website being diverted to a fraudulent site where customer details were harvested by the attackers
- Personal data of approximately 500,000 customers were compromised between June and September 2018
- A variety of information was compromised by poor security arrangements including login, payment card, travel details and name and address information

> *"People entrusted their personal details to BA and BA failed to take adequate measures to keep those details secure.*
> *Their failure to act was unacceptable and affected hundreds of thousands of people, which may have caused some anxiety and distress as a result. That's why we have issued BA with a £20m fine –* ***our biggest to date****.*
> *When organisations take poor decisions around people's personal data, that can have a real impact on people's lives.* ***The law now gives us the tools to encourage businesses to make better decisions about data, including investing in up-to-date security****."*
>
> Elizabeth Denham

Compensation

- Individuals have a right to claim compensation for damages caused by infringement of the Regulation from the Data Controller or Data Processor
- In October 2019, the High Court approved a Group Litigation Order against British Airways
  - Claimants have 15 months to take action
- Over 500,000 people now the right to join one of many lawsuits filed by law firms
- The October 2019 decision in Lloyd v Google by the Court of Appeal supports this approach

ICO and Marriott

- On 30 October 2020, the ICO fined Marriott International £20m under GDPR
  - 339 million guest records globally were exposed
  - 30 million related to residents of 31 EEA countries
  - 7 million related to UK residents
- The vulnerability began when the systems of the Starwood hotels group were compromised in 2014 and remained undetected until 2018
- Marriott subsequently acquired Starwood in 2016 and failed to undertake sufficient due diligence or do enough to secure its systems

*"The GDPR makes it clear that organisations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and **putting in place proper accountability measures** to assess not only what personal data has been acquired, but also how it is protected.*

***"Personal data has a real value so organisations have a legal duty to ensure its security**, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public."*

Elizabeth Denham

Recent ICO actions

Linda Reeves

- Accessed sensitive medical records of colleagues and people she knew without the consent of the data controller
- Fined £700, ordered to pay costs of £364.08 and a £70 Victim Surcharge

> *"Employees, who in many cases are very experienced and capable are getting into serious trouble and often losing their jobs, usually over little more than personal curiosity"*
> ICO

Kevin Bunsell

- Accessed his employer's recruitment system and emailed the personal information of 9 rival shortlisted candidates to his partner
- Included the name, address, telephone number and CV of each candidate
- When discovered he resigned and his wife, whose application was initially successful, was dismissed
- Fined £660, ordered to pay costs of £713.75 and a victim surcharge of £66

> *"Not respecting people's legal right to privacy can have serious consequences, as this case demonstrates. Not only might you face a prosecution and fine, along with the attendant publicity, but you may also lose your job and severely damage your future career prospects. People who supply their personal information to an organisation in good faith, such as when applying for a job, have a legal right to expect it will be treated lawfully and ethically."*
> ICO

Data sharing code of practice

- Published on the 17 December 2020
- The code, and a suite of new resources, provides practical advice to businesses and organisations on how to carry out responsible data sharing
- Information Commissioner 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

Age appropriate design – what does it mean in practice?

- ICO has launched a data sharing information hub with 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, 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

Data sharing code of practice

Elizabeth Denham

"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."
ICO

ACTION POINT

Ensure senior management are aware of class action lawsuits and review methods for mitigation such as insurance.

Session 5: Marketing

Adtech

- ICO engaged with the advertising industry throughout 2019
- A number of consultations were hosted by the ICO resulting in an interim report 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 were deemed to be generally immature, lacked detail and did not follow the ICO's recommended steps to assess the risk to the rights and freedoms of the individual
- As a result, the Internet Advertising Bureau (IAB) agreed a range of principles and is developing its own guidance for organisations on security, data minimisation and data retention
- Google will remove content categories and improve its process for auditing counterparties
  - It has also recently proposed improvements to its Chrome browser, including phasing out support for third party cookies within the next two years
- UK advertising trade bodies have agreed to produce guidance for their members

"The most effective way for organisations to avoid the need for further regulatory scrutiny or action is to engage with the industry reform and transformation, and to encourage their supply chain to do the same. I am both heartened at how much progress we have made, and disappointed that there are some who are still ignoring our message. Those who have ignored the window of opportunity to engage and transform must now prepare for the ICO to utilise its wider powers."

Simon McDougall- Executive Director for Technology and Innovation at the ICO

ICO – Draft marketing code of practice

- Consultation 19 December 2019 - 4 March 2020
- The draft code of practice aims to…
  - Provide practical guidance
  - Promote best practice for processing data for direct marketing purposes in compliance with data protection and e-privacy rules
- The draft code takes a life-cycle approach to direct marketing
  - Definition of direct marketing – does the code apply to you?
  - Planning your marketing, collecting data, delivering your marketing messages and individuals rights

Cookies and online tracking technologies – CNIL draft code of practice

Launched in January 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…
  - 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

Recent EU cases – The Netherlands

- March 2019 - the Dutch DPA issued new guidance and wrote to a number of organisations instructing them to remove 'cookie walls' as they were in breach of the GDPR
- Internet visitors must be asked for permission in advance for any tracking software to be placed

> *"Permission is not 'free' if someone has no real or free choice. Or if the person cannot refuse giving permission without adverse consequences."*

Recent EU cases – Belgium

- December 2019 - the Belgian Supervisory Authority imposed a €15,000 fine on Jubel.be - a legal information website operator
- Failure to provide sufficient information to users about the cookies deployed on its website
- Also for failing to obtain proper, opt-in consent for cookies

ACTION POINT

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

Session 6: COVID-19

Compliance – the ICO regulatory approach

- Will continue to recognise rights and protections granted to individuals by the law, but it will be more flexible during the crisis
- Will take into account the impact of the current situation when considering failure report data breaches
  - Continue to report personal data breaches without undue delay and within 72 hours of becoming aware of it
- Statutory timescales can't be extended but will take into account the impact of the pandemic on the ability to respond to data subject requests

Processing special category data

To process special personal data you must have a legal basis under Article 6 **AND** meet one of the conditions in Article 9

a) The Data Subject has given explicit consent to the processing for one or more specified purposes
b) To meet obligations or exercise rights under employment or social security laws
c) Preventive or occupational medicine
d) Public interest in the area of public health

Processing special category data

b) To meet obligations or exercise rights under employment or social security laws
   - Companies must take reasonable steps to look after the health, safety and welfare of staff - requirement under the Health and Safety at Work Act 1974
   - Limit as to what information employers should try to collect about its employees or visitors for the purposes of health and safety
   - Additional requirements under the Data Protection Act 2018

Workplace testing

- Special category data will require an Article 9 condition
  - ICO has identified 9(2)(b) as the most appropriate -employment obligations
  - Schedule 1 condition 1 of the Data Protection Act 2018 will apply alongside GDPR article 9
  - DPA 2018 Part 4 of Schedule 1

- Testing falls under legitimate interests provided there is sufficient reason
- COVID-19 - the legitimate interest is to prevent the spread of infectious diseases and to ensure workplace safety
- Document your Legitimate Interest Assessment

Workplace testing

- Employers should ensure the scope of health data collected and processed is limited to the minimum necessary and directly linked to any typical symptoms of the Coronavirus
- Justified by health and safety obligations placed on employers by the Health and Safety at Work Act 1974
- DPA 2018 requires an "appropriate policy document" and Records of Processing Activity (Article 30 GDPR) will also need to be updated

Employee health data relating to COVID-19 symptoms

Collection of data…

- Should be within the reasonable expectation of employees
- Well aligned with the employees' individual interests for their well-being
- Unlikely to be overriding compelling individual rights that would invalidate the processing

Session 7: Conclusion

Summary

- Review changes following Brexit and update documents and procedures where necessary
- Review international transfers and ensure new rules are being followed
- Ensure you can demonstrate accountability
- Can you demonstrate that you are following the six core principles?
- ICO Accountability Toolkit now released
- Beware strict interpretation of Article 14 – Bisnode
- Ensure you are following new DPIA guidance from the ICO
- New guidance on dealing with Subject Access Requests now released by the ICO
- Review your data breach processes and procedures to ensure compliance with ICO guidance
- Fines for breaches are now increasing rapidly across the EU
- Class action lawsuits may be a bigger concern for larger organisations
- Review the data sharing code of practice and adopt guidance where appropriate
- Electronic marketing guidance issued by many EU data protection authorities in 2019 and 2020
- Rules on cookies have now changed – does your website(s) comply?
- New rules for various advertising technologies (Adtech) issued across the EU
- Browser developers are changing the way cookies operate
- ICO direct marketing guidance released in 2020

Recommended actions

- Review current procedures against the accountability principle and ensure compliance can be demonstrated
- Review DSAR procedures in light of recent cases and ICO guidance
- Ensure senior management are aware of class action lawsuits and review methods for mitigation such as insurance
- Review use of cookies and other advertising technology and ensure use is compliant with revised guidance and developing case law
- Identify transfers from the EU and determine appropriate form of safeguarding

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

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

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