UKTraining

Data Mapping and Impact Assessments

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

Data Mapping and Impact Assessments

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

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

Contents

Part 1: GDPR Update

The new data protection landscape

Brexit

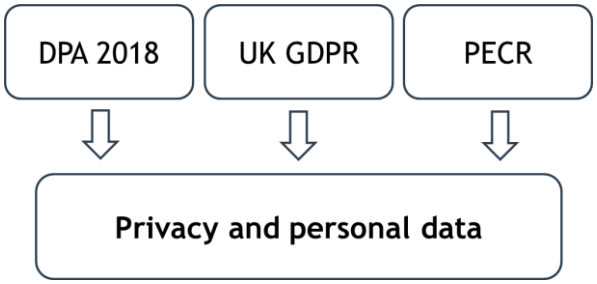
- The UK has left the EU and is no longer regulated domestically by the EU GDPR
- The UK now has the UK GDPR (United Kingdom General Data Protection Regulation)
  - Created by the European Union (Withdrawal) Act 2018
  - Updated by the Data Protection, Privacy and Electronic Communications (Amendments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

Brexit and the UK GDPR

- The UK GDPR is established 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



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

Data transfers

- 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

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

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

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 a key risk areas
- Note the ICO's insistence on robust and well-documented risk assessments and its recommendation to conduct DPIAs, even when conducting a DPIA is 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, 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

"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

ACTION POINT

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

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.**"

Elizabeth Denham, 25 May 2019

"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

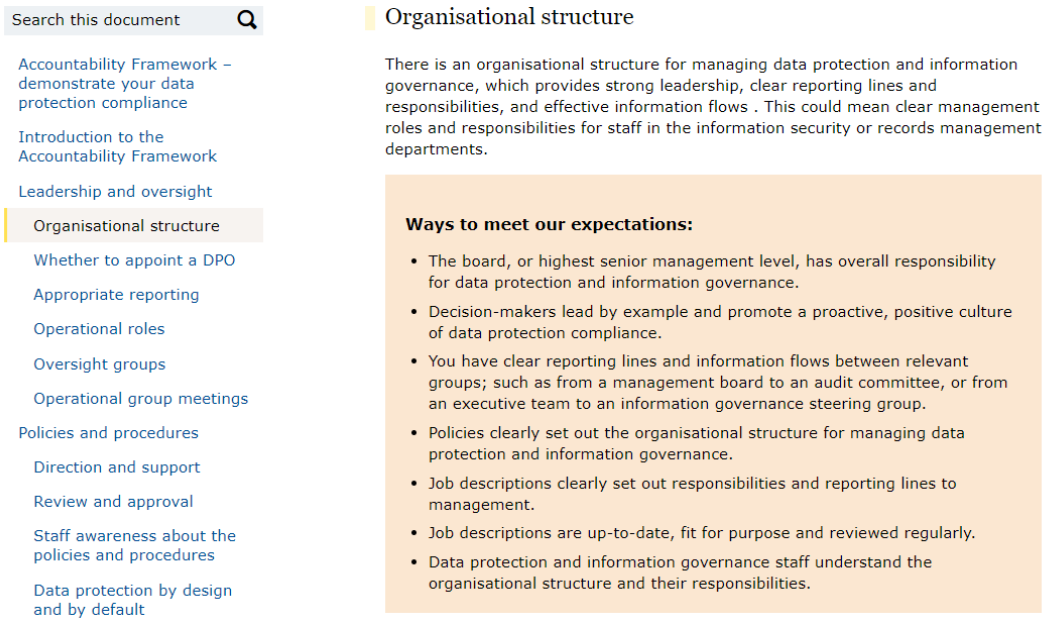
ICO accountability toolkit

- 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

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

ICO accountability toolkit categories



ACTION POINT

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

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

No Win No Fee?

- Individual's P45 was sent to an old address by mistake
- Individual had confirmed new address details previously
- The complaint was taken to a solicitors advertising 'no win no fee' services in relation to data breaches
- Claim was eventually settled for £1,800 to the claimant
- Legal fees for lawyers representing the Trust were £2319.50
- Legal fee for lawyers representing claimant were £8950
- Total costs of £13,038.50

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

ACTION POINT

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

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

Part 2: Data Protection Impact Assessments (DPIA)

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)

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

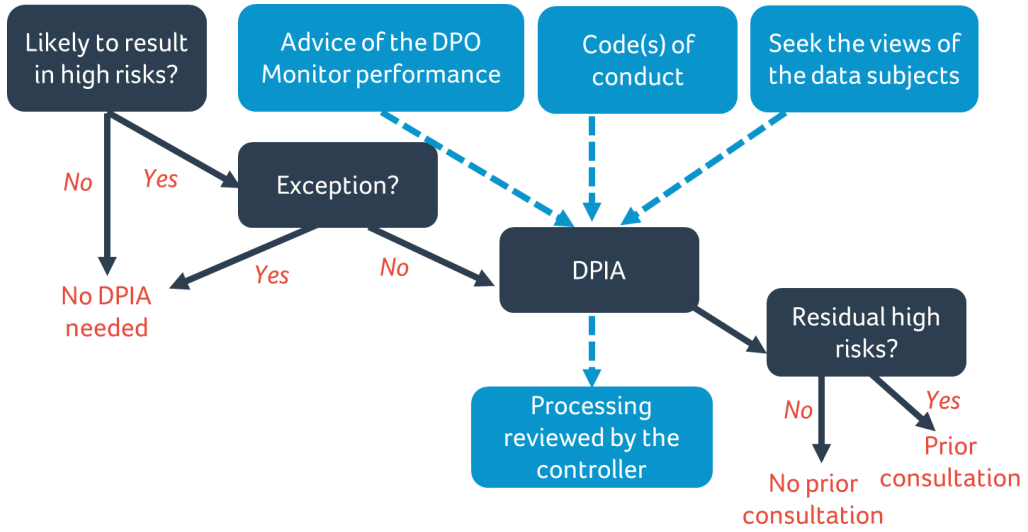
Swedish DPA response…

- 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

What are the basic principles of a DPIA?

It may concern a single process or multiple linked processes



EDPB guidance

The European Data Protection Boards (EDPB) published the following indicators of High Risk…

- Evaluation or scoring
- Automated decision-making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organisational solutions
- Preventing data subjects from exercising a right or using a service or contract

Advising on and monitoring Data Protection Impact Assessments

A DPIA is mandatory for the following types of processing

- Article 35(3)
  - Systematic and extensive profiling with significant effects
  - Large scale use of sensitive data
  - Public monitoring
- ICO mandated
  - New technologies
  - Denial of service
  - Large-scale profiling
  - Biometric
  - Genetic Data
  - Data matching
  - Invisible processing
  - Tracking
  - Targeting of children or other vulnerable individuals
  - Risk of physical harm

ICO example 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

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

ICO guidance - marketing

- Direct Marketing Code of Practice - 'direct marketing' activity which involves the processing of personal data that is likely to result in 'high risk' to the individual requires a DPIA before you start processing
  - When conducting 'large scale' profiling of individuals for marketing purposes
  - Matching datasets for marketing purposes
  - Processing which may be 'invisible' to the data subject
  - Using geo-location data for marketing purposes
  - Tracking the behaviour of individuals including online advertising, web and cross device tracking, tracing services (tele-matching & tele-appending), wealth profiling and loyalty schemes

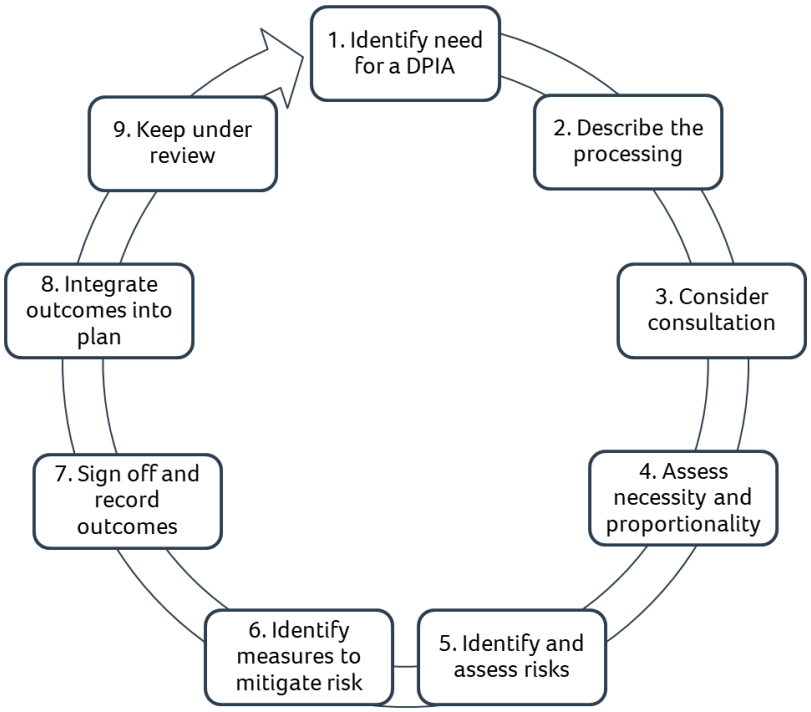
ICO guidance – data sharing

- Good practice to carry out a DPIA if you have a major project that involves disclosing personal data
- If you are confident that the type of data sharing you have in mind is unlikely to result in high risk, you are not legally required to carry out a DPIA
- ICO recommend carrying out a DPIA even when not legally obliged to do so as the process will help you to fully understand…
  - Whether you can share the data at all
  - Whether you can share the data, but with steps to mitigate the risks

Screening checklist

- Go to **uktraining.com/21dps** to download the template

DPIA templates



Source: ICO

ICO template

- ICO template can be downloaded from… ***www.uktraining.com/18tdp***
- Word document is a starting point and should be adapted to the needs of your organisation
- EDPB has also published guidance on acceptable DPIA's which the ICO template follows… ***www.uktraining.com/18wdp***

What is the purpose of a DPIA?

- The DPIA is an important aspect of the Accountability principle and should…
  - Describe exactly what processing is to take place
  - Assess the necessity and proportionality of the processing
  - Assess the risks to the rights and freedoms of Data Subjects
  - Recommend measures to mitigate any identified risks
- **It is intended to build and demonstrate compliance**

Internal awareness

- Key team members need to have the skills to conduct a DPIA:
  - Understanding of the process
  - Ability to brief key stakeholders
  - Explaining different types of risks
- If people don't what a DPIA is they may not consider the potential data protection issues
- Embedding DPIA's into your project lifecycle is highly recommended
- Make sure people who work on projects which involve personal data complete screening questionnaires as soon as possible

DPIA reviews

- Keep revisiting your DPIA
- Throughout the different stages of a project keep an ongoing dialogue with stakeholders, especially with Agile projects which may expand over time
- Check if new ideas, new developments have an impact

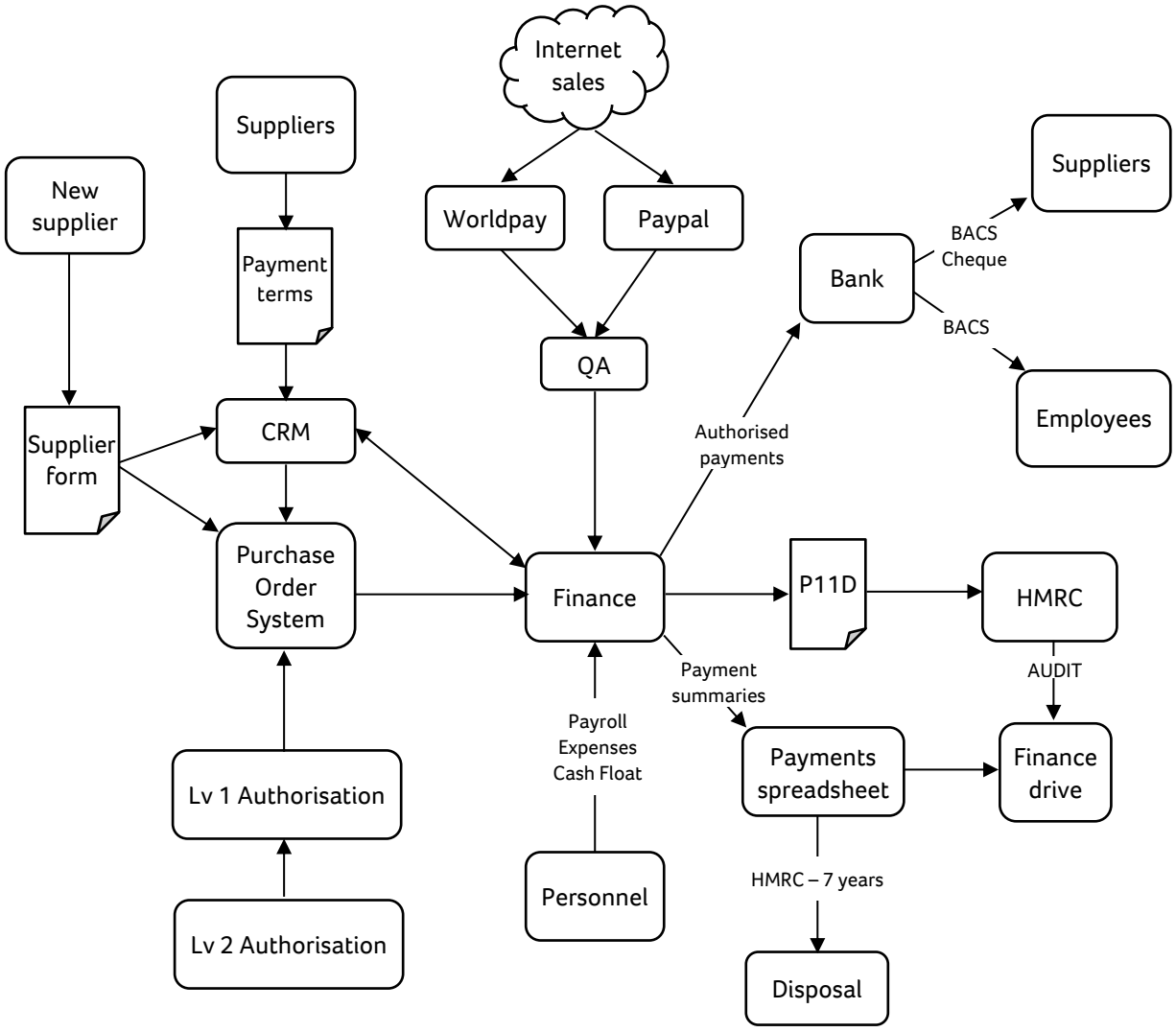
Identifying risks

- Risk should be viewed from the perspective of the data subjects
- Consider risks of identity theft or fraud, financial loss, reputational damage, loss of confidentiality, significant economic or social disadvantage, etc
- Identify sources of risk and analyse potential impact on the data subjects
- Any significant possibility of very serious harm may still be enough to qualify as a high risk
- Equally, a high probability of widespread but more minor harm may still count as high risk

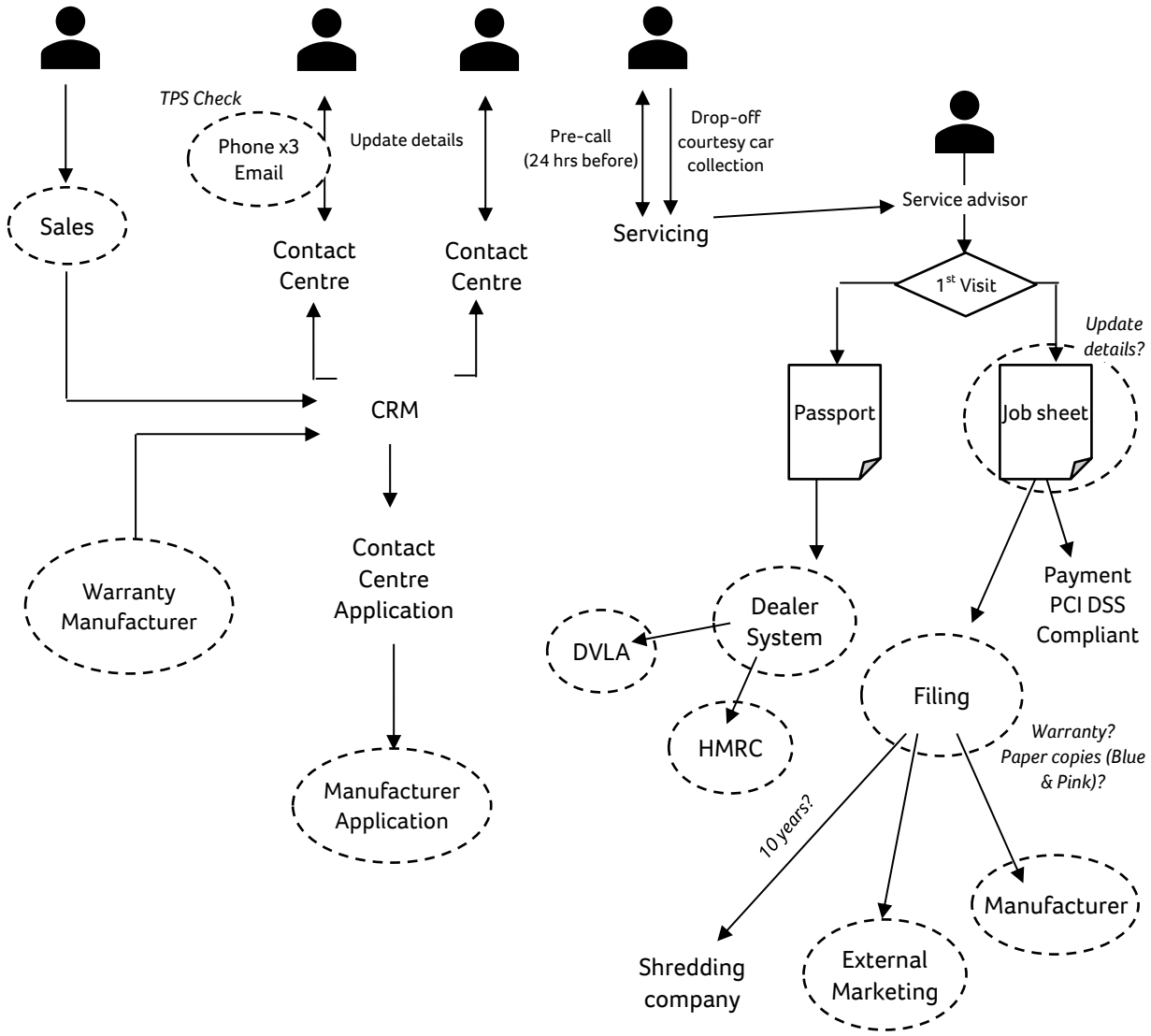
- Any significant possibility of very serious harm may still be enough to qualify as a high risk
- Equally, a high probability of widespread but more minor harm may still count as high risk

Severity of impact				
	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Data flow mapping – example 1



Data flow mapping – example 2



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
- ICO Accountability Toolkit now released
- Class action lawsuits may be a bigger concern for larger organisations
- Review the data sharing code of practice and adopt guidance where appropriate
- Create a DPIA screening questionnaire
- Create a list of project types that will require a DPIA
- Create a DPIA template that is simple to understand
- Define DPIA procedures and document them
- Ensure key staff are aware and trained
- Build DPIA's into the early stages of project lifecycles
- Review DPIA's and refine procedures and supporting templates
- Embed DPIA's into your accountability processes

Recommend actions

- Identify transfers from the UK and determine appropriate form of safeguarding
- Review current procedures against the accountability principle and ensure compliance can be demonstrated
- Ensure senior management are aware of class action lawsuits and review methods for mitigation such as insurance
- Define and document a DPIA procedure and support with template documents
- Ensure awareness and training in your DPIA procedures

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

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